REGOLAMENTO PRIVACY
DI OSCULATI &PARTNERS SRL

Regole di comportamento riguardanti il trattamento dei dati personali e aziendali, degli strumenti e dei sistemi informatici.

I. INTRODUZIONE

1. PREMESSA

Osculati & Partners Srl – di seguito anche solo O&P, con sede legale e operativa in Milano, Piazza San Sepolcro n. 1, nello svolgimento delle sue attività, raccoglie e tratta dati personali di clienti, fornitori, collaboratori e terzi.

La stessa riconosce l'importanza dei principi fissati dalle norme in materia di privacy e inerenti alla necessità, liceità, proporzionalità del trattamento e garantisce di attuare ed adottare procedure interne e misure idonee ed adeguate a proteggere la riservatezza dei dati personali dei suoi utenti.

Ad oggi riconosciuto il moltiplicarsi delle attività illecite attuabili con tali strumenti e la pericolosità che attacchi dall'esterno ed usi impropri e/o illegali anche dall'interno possano mettere a rischio i dati che si gestiscono e ciò a scapito dell'azienda, in lesione dei diritti degli utenti.
Le conseguenze di tali azioni illecite possono andare dalla riduzione delle funzionalità alla perdita o alterazione dei dati alla realizzazione di fattispecie di reato o comunque di illeciti, con la conseguente applicazione di severe sanzioni amministrative e/o condanne penali.

Per tali motivi, nonché con l'obiettivo di mantenere un equilibrio tra la tutela della privacy ed il libero flusso delle informazioni e per far maturare nel personale e nei collaboratori la consapevolezza dell'importanza dei dati da loro trattati, O&P ha deciso di redigere il presente Regolamento privacy con conseguente regolamento informatico e linee guida all'uso degli strumenti informatici e telematici.
Il presente Regolamento si prefigge altresì l'obbiettivo di preservare la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni a tutela della dignità delle persone fisiche, delle libertà fondamentali e del valore del capitale intellettuale di O&P.

Questo l'obiettivo principale del presente Regolamento che si inserisce nel contesto della generale disciplina in materia di Privacy e nel sistema normativo che regola l'organizzazione, i processi e le funzioni di O&P.
Le risorse informatiche e telematiche messe a disposizione della O&P costituiscono uno dei suoi punti di forza, ma nello stesso tempo possono essere fonte di rischio per la sicurezza delle informazioni trattate e per l'immagine i O&P.
Per questo motivo il loro utilizzo deve sempre ispirarsi a criteri di liceità, correttezza e trasparenza.

L'individuazione di regole precise e chiare per l'utilizzo dei sistemi informatici e il trattamento dei dati personali e aziendali d i O&P rappresenta un passaggio obbligato per assicurare una ottimale gestione delle funzioni aziendali.

Sono questi gli elementi che, nel contesto della disciplina in materia di privacy, hanno determinato O&P ad elaborare ed adottare il presente Regolamento, che sostituisce ed integra la precedente policy privacy.

1.2 IL TRATTAMENTO DEI DATI

Per ciò che attiene al trattamento dei dati personali, O&P dichiara che è effettuato in conformità alle finalità da lei previste e dichiarate.
I trattamenti dei dati personali e/o personali sensibili sono relativi alla raccolta, registrazione, organizzazione, consultazione, elaborazione, modificazione, selezione, estrazione, archiviazione, cancellazione e distruzione.
Tali operazioni vengono fatte sia con strumenti manuali (è il caso dei dati negli archivi cartacei), sia con strumenti informatici (naturalmente per i dati su supporto informatico) presso la sede del titolare, con l'utilizzo e l'archiviazione in server di sua proprietà, locati presso la sede.

Per assicurare la corretta gestione e trattamento dei dati acquisiti e per aumentare la consapevolezza sulla delicatezza di tale attività, La O&P svolge (anche con cadenza periodica) le seguenti azioni:

- Aggiornamento del *Regolamento informatico e linee guida* per attuare una idonea politica della privacy e poter fornire garanzia agli interessati sul conforme trattamento dei dati.
- Formazione del personale in materia di Privacy.
- Adeguamento del sistema informativo (SIA) ed aggiornamento costante dello stesso.
- Aggiornamento nomine degli incaricati con definizione delle mansioni relative al trattamento dei dati personali e/o personali sensibili (anche per gruppi omogenei), responsabile del trattamento ed amministratore di sistema.

2. TUTELA DEL LAVORATORE

Il luogo di lavoro è una formazione sociale rispetto alla quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità di ciascuno in modo da garantire, in una cornice di reciproci diritti e doveri, l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali.

3. SCOPO, CAMPO DI APPLICAZIONE E DESTINATARI DEL PRESENTE REGOLAMENTO

Lo scopo del presente Regolamento è quello di definire un insieme di norme comportamentali a cui tutti i dipendenti, i collaboratori, le eventuali terze parti e – in generale- gli utenti interni ed esterni che operano per O&P devono uniformarsi nell'ambito delle attività che implicano un trattamento di dati ed informazioni.

Il presente Regolamento è realizzato in conformità a quanto previsto dal Decreto Legislativo n. 193/2003 – Codice in materia di protezione dei dati personali, dal Regolamento Europeo n. 2016/679 – General Data Protection Regulation (da ora "GDPR") e dai Provvedimenti del Garante.

Il presente Regolamento è destinato ai seguenti utenti (da ora "utenti"):

Utenti interni:

- Componenti degli Organi statutari;
- Dipendenti
- Collaboratori coordinati e continuativi
- Personale presente in O&P a fronte di accordi di distacco o di comando
- Consulenti e collaboratori occasionali
- Affiliati

Utenti esterni:

- Collaboratori a qualsiasi titolo di imprese fornitrici di beni, servizi o lavori che realizzano opere in favore di O&P;
- Personale di altre entità presenti in O&P vin forza di convenzioni o accordi inter-istituzionali;
- Visitatori ed ospiti di vario genere.

II DEFINIZIONI

1. Sono qui di seguito riportate le principali definizioni privacy trattate dal GDPR:

Dato personale: qualsiasi informazione che identifica o rende identificabile una persona fisica e che può fornire dettagli sulle sue caratteristiche fisiche, fisiologiche, genetiche o psichiche, sulle sue abitudini, sul suo stile di vita, sulle sue relazioni personali, sul suo stato di salute o sulla sua situazione economica.
Dati identificativi: dati personali che permettono l'identificazione diretta di una persona fisica.
Dati sensibili: dati personali idonei a rivelare lo stato di salute (attinenti alla salute fisica o mentale, compresa la prestazione di servizi di assistenza sanitaria), e la vita sessuale, 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 di una persona fisica.
Dati genetici: dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla sua fisiologia o salute.

Dati biometrici: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati giudiziari: dati idonei a rilevare informazioni riguardo provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Trattamento di dati personali: qualsiasi operazione compiuta con o senza l'ausilio di processi automatizzati e applicata a dati personali, o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, 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.

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali che consiste nell'utilizzo di tali dati 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.

Pseudonimizzazione: trattamento dei dati personali effettuato in modo tale che tali dati non possano più essere attribuibili ad 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 i dati personali non siano attribuibili a una persona fisica identificata o identificabile.

Comunicazione di dati personali: dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in base ad una precisa finalità ed una modalità certa e sicura di trattamento, anche mediante la loro messa a disposizione o consultazione.

Diffusione di dati personali: dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Violazione di dati personali: 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.

Titolare del trattamento: organizzazione nel suo complesso, nella persona del suo Legale Rappresentante che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Contitolare del trattamento: Titolare del trattamento che determina congiuntamente ad altro Titolare le finalità e i mezzi del trattamento in modo trasparente e mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR.

Responsabile del trattamento (interno o esterno): persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento. Il Responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

Sub-responsabile del trattamento: persona fisica o giuridica, autorità pubblica, servizio o altro organismo alla quale un Responsabile del trattamento ricorre per l'esecuzione di specifiche attività di trattamento per conto del Titolare;

Incaricato/autorizzato del trattamento: persona fisica autorizzata a compiere operazioni di trattamento dati, sulla base dei regolamenti adottati dal Titolare e delle istruzioni impartite dal Responsabile del trattamento.

Interessato: persona fisica cui si riferiscono i dati personali trattati.

Amministratore di sistema: persona fisica nominata dal Titolare e preposta alla gestione e sicurezza dei sistemi informativi attraverso l’applicazione delle misure necessarie al mantenimento della riservatezza, disponibilità e integrità del dato personale trattato nei sistemi informativi.

Responsabile della protezione dei dati (Data Protection Officer - DPO): persona fisica nominata dal Titolare che, ai sensi degli artt. 37-39 del succitato GDPR, operando in modo indipendente rispetto all'organizzazione, consiglia il Titolare riguardo obblighi, requisiti ed evoluzione normativa, realizza verifiche interne sulla corretta applicazione delle disposizioni normative e del sistema di gestione privacy definite dal Titolare, assiste il Titolare sulla valutazione di impatto privacy e sull'analisi del rischio e rappresenta il punto di contatto per interessati e Garante Privacy.

Sono inoltre riportate per completezza alcune altre definizioni utili alla corretta gestione dei processi di trattamento dei dati personali.

Badge: tesserino con chip elettronico di riconoscimento.
Pass: tesserino cartaceo senza identificativo.
Strumenti informatici: stampanti, laptop, computer da tavolo, telefoni fissi, smartphone, tablet, e-book reader, telecamere IP, e, in generale, qualsiasi dispositivo in grado di connettersi a una rete IP.
Data Center: locale ad accesso limitato che ospita i server, i sistemi di calcolo e i dispositivi di networking, oltre che i sistemi di storage su cui sono residenti i dati.
Cloud Pubblica: modello di conservazione dati su computer in rete dove i dati stessi sono memorizzati su molteplici server virtuali generalmente ospitati presso strutture di terze parti o su server dedicati.

III. MODELLO ORGANIZZATIVO

1.CLASSIFICAZIONE DELLE INFORMAZIONI IN O&P

O&P classifica il proprio patrimonio informativo (costituito da tutti i dati e le informazioni trattati nei diversi processi, tra i quali anche i dati personali) secondo i seguenti criteri:

Dati e informazioni pubbliche: sono le informazioni liberamente trattabili da Utenti attraverso i mezzi di comunicazione messi a disposizione da

O&P (sito internet, pubblicazioni, comunicati, ecc.). Queste informazioni non richiedono da parte dell'Utente particolari attenzioni di riservatezza. La divulgazione di tali informazioni non presenta implicazioni per O&P in quanto si tratta di informazioni pubbliche che possono essere diffuse.

Dati e informazioni interne: sono le informazioni che possono essere trattate dagli Utenti esclusivamente all'interno dei processi e del contesto organizzativo di O&P attraverso i canali istituzionali messi a disposizione dalla società (e-mail, intranet, sito internet, aree di scambio su server e computer, ecc.). Queste informazioni richiedono da parte dell'Utente una particolare attenzione nel trattamento, in quanto la loro divulgazione rappresenta una violazione dei vincoli di riservatezza ai quali è legato ogni Utente con un possibile impatto legale (per esempio, violazione della privacy), a meno di essere rielaborate in modo da essere declassate a livello pubblico.

Dati e informazioni riservate: sono le informazioni che possono essere trattate da gruppi di Utenti autorizzati in virtù del ruolo e di una precisa finalità di trattamento individuata dal Titolare o dal Responsabile del trattamento. Tali informazioni devono essere comunicate solo ad Utenti legittimati, valutando lo strumento di comunicazione più appropriato messo a disposizione da O&P in quanto la loro diffusione può avere un rilevante impatto legale (per esempio, violazione della privacy), d'immagine e di competitività per O&P.

Dati e informazioni strettamente riservate: sono le informazioni che possono essere trattate esclusivamente da determinati Utenti in base al ruolo ed alle responsabilità ricoperte in O&P. La divulgazione di tali informazioni può produrre gravi danni legali (per esempio, violazione della privacy), di immagine e di competitività per O&P.

2. MODELLO ORGANIZZATIVO DI RESPONSABILITÀ PRIVACY

Nell'ambito della conformità al GDPR e sulla base del proprio organigramma, O&P ha definito e formalizzato un Modello Organizzativo di responsabilità privacy finalizzato al corretto trattamento dei dati personali. Il modello è allegato al presente Regolamento e ne costituisce parte integrante (**Allegato 1**).

Al di là del Modello Organizzativo relativo alle responsabilità privacy di cui sopra, tutti coloro che siano a capo di un'operazione che contempla il trattamento di dati personali - d'intesa con il Titolare, dovranno laddove si rendesse necessario valutare l'adozione di una *policy ad hoc*.

IV. POLICY DI COMPORTAMENTO

1. PRINCIPI GENERALI DEL TRATTAMENTO

Trattare un dato personale rappresenta qualunque operazione o complesso di operazioni realizzate su un dato personale ed effettuate anche senza l'ausilio di strumenti elettronici. Il trattamento di un dato personale, per essere lecito, corretto e trasparente, deve sempre avvenire secondo alcuni principi generali privacy, che possono essere considerati vincoli inscindibili al trattamento dei dati personali. È importante chiedersi sempre se questi vincoli siano rispettati e solo ad una risposta sempre positiva possiamo avere la certezza che la privacy di una persona sia rispettata. In particolare quando avviene un trattamento di dati personali devono sempre essere rispettati i seguenti principi generali:

1. **Il rispetto della dignità dell'interessato**, cioè della persona fisica di cui si stanno trattando i dati personali.
2. **Il rispetto dei principi di liceità, correttezza e trasparenza:** i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato, in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, distruzione o danno accidentali. Quanto alla trasparenza, tutte le informazioni destinate al pubblico o all'interessato devono essere concise, facilmente accessibili e di facile comprensione; il linguaggio utilizzato deve essere semplice e chiaro.
3. **Il rispetto del principio di limitazione della finalità:** gli scopi del trattamento devono essere determinati, espliciti e legittimi, e successivamente trattati in un modo che non sia incompatibile con tali scopi (salvi gli ulteriori trattamenti per finalità di archiviazione

nel pubblico interesse o per finalità di ricerca scientifica o storica, o per fini statistici).

4. **Il rispetto del principio di minimizzazione dei dati:** i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Nello specifico, i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'uso di dati personali, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possano essere realizzate mediante dati anonimi o altre opportune modalità che permettano di identificare l'interessato solo in caso di necessità (c.d.' *principio di necessità'*).
5. **Il rispetto del principio di esattezza**: i dati trattati devono essere esatti e, se necessario, aggiornati, pertanto devono essere adottate tutte le misure ragionevoli per cancellare o rettificare i dati inesatti rispetto alle finalità per le quali sono trattati.
6. **Il rispetto del principio di limitazione della conservazione**: i dati trattati devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario al conseguimento degli scopi per cui sono raccolti e trattati (salvo specifici obblighi di legge, trattamenti di archiviazione nel pubblico interesse o per finalità di ricerca scientifica o storica, o per fini statistici).
7. **Il rispetto del principio di integrità e riservatezza**: i dati devono essere trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti dalla perdita, dalla distruzione e dal danno accidentale.

2. TRATTAMENTO DI DATI RACCOLTI PER SCOPI DI RICERCA

Gli scopi di ricerca devono essere chiaramente determinati e resi noti all'interessato nell'informativa. I dati personali trattati per scopi di ricerca non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né per trattamenti finalizzati a scopi di altra natura. Essi sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo. I dati identificativi, qualora possano essere conservati, sono abbinabili ad altri dati, sempre che l'abbinamento sia temporaneo ed essenziale per i propri trattamenti.

Le disposizioni, relative alla riservatezza dei dati personali, non si applicano ai dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

3. GESTIONE DEI LOCALI E DELLE RISORSE FISICHE

Tutti i locali e tutte le risorse fisiche di O&P devono essere utilizzati e custoditi con la massima diligenza al fine di garantire un'efficiente conduzione dell'attività lavorativa ed un adeguato livello di sicurezza delle informazioni, attenendosi al presente Regolamento per garantire la sicurezza fisica di aree ed *asset* di O&P.

4. ACCESSO AGLI UFFICI ED AREE PROTETTE

Sede e uffici. L'accesso agli uffici, alle aree protette, alle aree riservate ed agli archivi cartacei, è permesso agli Utenti autorizzati muniti di badge personal e/o chiave di accesso, in base a precise e motivate esigenze lavorative.

Ulteriori e specifici accessi ad uffici ed aree protette potranno essere concessi e abilitati da parte solo a seguito di preventiva e motivata richiesta da parte dei vari rispettivi Responsabili.

I visitatori e gli ospiti di vario genere potranno avere accesso alle suddette aree di O&P esclusivamente previa registrazione e accompagnati da un Utente.

Locali Server. L'accesso ai locali Server di O&P è permesso esclusivamente a personale autorizzato.

In via eccezionale e per breve tempo, nel locale server è consentito l'accesso anche a visitatori e ospiti di vario genere, purché autorizzati e accompagnati da personale di O&P autorizzato. I visitatori e gli ospiti di vario genere dovranno essere adeguatamente istruiti dal personale autorizzato in merito alle caratteristiche dell'ambiente, ai rischi presenti, alle norme comportamentali previste e alle procedure da attuare per prevenire o gestire situazioni di emergenza e di rischio.

5. RIPRESE VIDEO-AUDIO-FOTOGRAFICHE ALL'INTERNO DI O&P

Qualsiasi ripresa video-audio-fotografica deve essere realizzata rispettando i diritti delle singole persone coinvolte.

Utenti interni: per ragioni connesse alla propria attività lavorativa le riprese video -audio-fotografiche devono essere autorizzate dal proprio Responsabile. Tali riprese possono essere utilizzate esclusivamente per finalità lavorative e non possono essere divulgate al di fuori del contesto istituzionale in cui sono state realizzate.

Al di fuori di questa casistica è vietato effettuare riprese video-audio-fotografiche in qualunque area di O&P, salvo preventiva e formale autorizzazione del proprio Responsabile.

Gli Utenti interni potranno essere fotografati e/o ripresi in occasione di eventi, seminari e momenti di formazione.

In questi casi, le immagini e le riprese potranno essere utilizzate per scopi e comunicazioni istituzionali.

Utenti esterni: è vietato effettuare riprese video-audio-fotografiche in qualunque area di O&P. Eventuali eccezioni devono essere autorizzate direttamente dalla O&P. L'Utente interno referente di eventuali visite è tenuto a far rispettare queste prescrizioni.

6. POSTAZIONI DI LAVORO

L'utilizzo della postazione di lavoro e il conseguente accesso ai documenti, atti e archivi è consentito nei limiti della propria funzione e dei propri incarichi.

Scrivania pulita. La propria scrivania deve essere mantenuta in ordine, verificando di non lasciare documenti e atti riservati senza un proprio controllo all'accesso di terzi, in momenti di pausa, terminata la giornata di lavoro e/o in periodi di assenza.

7. MISURE FISICHE DI CUSTODIA DI DOCUMENTI E ATTI CARTACEI

I dati cartacei ed i supporti cartacei necessari per lo svolgimento delle mansioni lavorative devono essere custoditi in armadi o cassettiere del contesto organizzativo in cui si opera. Tutti gli archivi sono ad accesso limitato, per cui è possibile accedervi nei limiti della necessità per prelevare e riporre i documenti necessari per lo svolgimento delle mansioni lavorative. I documenti dovranno essere riposti correttamente durante i periodi di temporanea assenza ed al termine dell'attività lavorativa negli appositi archivi.

Gli archivi di documenti e atti contenenti dati sensibili dovranno essere custoditi in armadi chiusi a chiave.

L'**eliminazione fisica** di ogni documento cartaceo o supporto informatico contenente dati e informazioni aziendali e/o personali deve essere effettuata solo utilizzando gli appositi strumenti.

Si raccomanda di non lasciare documenti incustoditi.

8. GESTIONE DEI DATI PERSONALI E AZIENDALI

Ogni Utente è responsabile dei dati e delle informazioni delle quali entra in possesso per lo svolgimento della sua attività lavorativa. Deve quindi trattare i dati e le informazioni adottando ogni idonea misura di sicurezza al fine di tutelarne la riservatezza, la sicurezza, l'integrità ed il corretto utilizzo.

I dati e le informazioni potranno essere comunicate a terze parti esclusivamente nell'ambito della propria funzione e secondo le finalità connesse alla propria attività lavorativa.

- vietata la comunicazione di dati e informazioni verso terzi che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale e del *know-how* ed alla redditività aziendale o che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro.

- assolutamente vietata la divulgazione a terzi di informazioni riservate, confidenziali o comunque di proprietà del Titolare. In caso di violazione, il Titolare si riserva di avviare i relativi provvedimenti disciplinari, nonché le azioni civili e penali consentite.

Si ricorda, inoltre, che la diffusione illecita di dati e informazioni potrebbe configurare, oltre alla violazione del presente Regolamento, la violazione di norme con conseguenze sia civili che penali a carico del responsabile dell'illecita diffusione, nonché come violazione della normativa che regola il rapporto di lavoro.

9. STRUMENTI INFORMATICI

L'utilizzo degli strumenti informatici in dotazione è di carattere professionale. In deroga a tale principio O&P autorizza un moderato e ragionevole utilizzo privato. Tale utilizzo deve essere limitato ed ispirato a criteri di buon senso e non dovrà ostacolare l'utilizzo professionale. Lo spazio dello strumento affidato utilizzato a fini "privati" (ad esempio dislocazione di file dati, foto o filmati), dovrà perciò essere limitato e non dovrà precludere e limitare quello dedicato all'utilizzo professionale.

Tutti gli strumenti dovranno essere bloccati e protetti da password, se lasciati incustoditi.

Gli strumenti dovranno essere automaticamente spenti o messi in modalità a basso consumo se non usati per più di un'ora, a meno di motivate esigenze di ricerca.

Gli Amministratori di Sistema sono gli unici ad avere accesso ai sistemi informatici gestiti collegati alle reti di O&P con privilegi di Amministratore o "root", sia locale che di rete.

Sulle reti di O&P e sui dispositivi gestiti centralmente, non è consentito modificare in alcun modo il sistema operativo o le applicazioni installate dagli Amministratori di Sistema che rispettano le misure idonee di sicurezza.

L'utilizzo dei dispositivi informatici è in ogni caso soggetto al rispetto del Regolamento e linee guida per un utilizzo sicuro delle reti. Si veda in tal senso pure l'allegato Documento sulla rete e protezione dei dati (**Allegato 2**).

10. CUSTODIA DEGLI STRUMENTI INFORMATICI

Gli strumenti informatici di proprietà di O&P devono essere custoditi dall'Utente con cura e diligenza prevenendo possibili danneggiamenti che ne compromettano il corretto funzionamento ed evitando di lasciarli incustoditi in ambienti pubblici.

In caso di furto o danneggiamento di beni, l'Utente dovrà informare immediatamente la O&P, il Servizio IT, e presentare formale denuncia alle autorità di pubblica sicurezza e consegnarne copia ai soggetti sopra menzionati per l'attivazione degli atti formali di scarico e di attivazione delle coperture assicurative.

11. GESTIONE DELLE CREDENZIALI DI ACCESSO E DELLE PASSWORD

Le credenziali di autenticazione per l'accesso alla rete e per altri servizi vengono assegnate dal Servizio IT, consegnate all'Utente da O&P; esse sono modificabili dall'Utente e consistono in un codice per l'identificazione dell'Utente (username), associato ad una parola chiave (password) riservata che dovrà venir custodita dall'Utente con la massima diligenza e non divulgata. Ogni Utente è personalmente responsabile della sicurezza e di qualunque operazione effettuata utilizzando le proprie credenziali. È proibito accedere alla rete e ai programmi con credenziali diverse dalle proprie o in maniera anonima.

Sulla base della normativa vigente, le password degli Utenti devono essere cambiate almeno ogni sei mesi. Le password degli Incaricati del trattamento di dati sensibili devono essere cambiate almeno ogni tre mesi.

12. GESTIONE E PROTEZIONE DEI DATI

L'accesso ai dati è consentito nei limiti della propria funzione organizzativa e della propria attività lavorativa.

I dischi di rete presenti sui server di O&P sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia inerente all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte del personale incaricato.

Si ricorda che i dischi o altre unità di memorizzazione locali non sono soggette a salvataggio da parte del personale incaricato. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo Utente.

Il personale incaricato può in qualunque momento procedere alla rimozione di ogni file o applicazione che reputerà pericolosa per la sicurezza sia sugli strumenti informatici degli Utenti, sia sulle unità di rete: di tale intervento ne è informato il suo diretto Responsabile.

Il **backup** dei principali server di rete viene effettuato dagli Amministratori di Sistema. Gli Utenti che trattengono dati di O&P in aree per cui non è previsto backup sono responsabili del salvataggio degli stessi e di eventuali danni a O&P o a terzi anche di natura civilistica causati dalla loro perdita o sottrazione.

Fermi restando i vincoli esistenti a tutela della privacy per il proprio personale, gli Utenti devono essere consapevoli che i dati da loro trattati sui sistemi informatici di O&P possono essere di proprietà di O&P o comunque sotto la responsabilità della stessa. Proprio per garantire la sicurezza e l'integrità delle informazioni presenti sui sistemi informatici aziendali, non è possibile garantire in maniera assoluta, in caso di controlli, la segretezza delle informazioni.

La memorizzazione temporanea di dati su strumenti informatici privati è consentita a patto che i suddetti strumenti siano protetti in modo da non consentire l'accesso di estranei non autorizzati.

È vietato il salvataggio di dati e informazioni di carattere aziendale in sistemi di ***cloud pubblica*** non autorizzati dagli Amministratori di Sistema.

13. GESTIONE DELLA POSTA ELETTRONICA

L'assegnazione di una casella di posta elettronica di O&P (da ora "e -mail O&P") è di carattere professionale. In deroga a tale principio O&P autorizza un moderato e ragionevole utilizzo privato. Tale utilizzo deve essere limitato ed ispirato a criteri di buon senso e non dovrà ostacolare l'utilizzo professionale. Lo spazio della risorsa affidata utilizzato a fini "privati" dovrà perciò essere limitato e non dovrà precludere e limitare quello dedicato all'utilizzo professionale.
O&P, in conformità alla disciplina in materia di privacy, prevede che ad ogni messaggio in uscita sia automaticamente aggiunto un breve testo di avviso al ricevente della natura potenzialmente riservata del messaggio.

Gli Utenti dell'e-mail O&P sono responsabili dell'utilizzo della stessa e devono mantenere un corretto comportamento nell'utilizzo della posta elettronica. In particolare, gli Utenti devono seguire le seguenti disposizioni:

- non inviare né conservare messaggi di posta elettronica e/o allegati dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico o comunque inappropriato o illegale, salvo specifiche esigenze di ricerca;

- prestare la massima attenzione nell'inoltro di e-mail riportanti contenuti e indirizzi e-mail di precedenti comunicazioni;

- prestare la massima attenzione ad e-mail sospette, avvisando l'Amministratore di Sistema in caso di dubbi sulla provenienza/contenuto delle stesse;

- creare una sezione denominata “Posta personale” all’interno della propria casella di posta, alla quale gli Amministratori di Sistema non potranno accedere se non per gravi motivi di sicurezza informatica.

Per motivi di sicurezza informatica ed in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all’attività lavorativa, l’accesso alla casella di posta dell’Utente potrà essere gestita dagli Amministratori di Sistema su richiesta del Responsabile del Trattamento dell’Utente al fine di verificare il contenuto dei messaggi e ad inoltrare al Titolare del Trattamento quelli ritenuti rilevanti per lo svolgimento dell’attività lavorativa.

La **Posta Elettronica Certificata (PEC)** può essere utilizzata dagli Incaricati solamente per motivi professionali.

15. UTILIZZO DELLA NAVIGAZIONE INTERNET

L’accesso a Internet è fornito principalmente per scopo professionali, per accedere a informazioni e contenuti necessari allo svolgimento dell’attività lavorativa. Essendo uno strumento di lavoro, gli Utenti cui si attribuisce l’accesso, sono responsabili del suo corretto utilizzo. Come per la posta elettronica, O&P ne autorizza un moderato e ragionevole utilizzo privato, limitato ed ispirato a criteri di buon senso senza ostacoli all’attività professionale.

Il numero e la durata degli accessi a Internet sono costantemente registrati. La consultazione di tali registrazioni può avvenire solo in forma anonima e aggregata salvo i casi previsti dalla legge e dal mancato rispetto del presente Regolamento. Gli eventuali controlli compiuti dagli Amministratori di Sistema potranno avvenire mediante un sistema di analisi dei file giornale. Gli Utenti devono seguire le seguenti regole di navigazione della rete Internet:

a. è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore, che siano essi appartenenti a persone o aziende, coperti da copyright, brevetto o proprietà intellettuale, ivi compresa l’installazione o la distribuzione di software che non sia specificatamente licenziato per essere utilizzato all’interno di O&P;

b. è tassativamente vietato navigare siti e scaricare materiale pericolosi/vietati o aventi contenuti illegali (contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico, pedopornografico, terrorismo o comunque inappropriato o illegale), salvo specifiche esigenze di ricerca;

c. è vietato effettuare copia non autorizzata di materiale coperto da copyright compreso ma non limitato a digitalizzazione e distribuzione di foto da riviste, libri o altre fonti, musica o materiale video;

d. è vietato utilizzare l'infrastruttura tecnologica di O&P per procurarsi e diffondere materiale in violazione con le normative vigenti;

e. è vietato effettuare attività che possano generare dei problemi di sicurezza o danneggiare le comunicazioni sulla rete;

f. è vietato eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all'host dell'Utente (sniffing) a meno che questa attività non faccia parte dei compiti dell'Utente e quindi formalmente autorizzata dagli amministratori di sistema;

g. è vietato aggirare le procedure di autenticazione o la sicurezza di qualunque host, rete, account.

15. ACCESSO INTERNET PER UTENTI ESTERNI

È previsto un sistema per consentire l'accesso e la navigazione in Internet ad Utenti esterni. Il numero e la durata degli accessi ad Internet sono costantemente registrati.

16. ACCESSO DA REMOTO - VIRTUAL PRIVATE NETWORK (VPN)

L'accesso dall'esterno alla rete di O&P è consentito esclusivamente attraverso precise modalità di connessione sicura. Ogni altro accesso è espressamente vietato.

17. COMUNICAZIONE DI DATI E INFORMAZIONI ATTRAVERSO SOCIAL MEDIA

È assolutamente vietato pubblicare in internet attraverso social media personali, forum, chat, blog, siti internet, dati ed informazioni di carattere aziendale (informazioni, documenti, appunti, commenti personali o di terzi, foto, video, audio, ecc..) che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale e del know-how ed alla redditività di O&P o che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro.

È assolutamente vietato divulgare notizie false.

E' invece autorizzata la divulgazione di informazioni già rese pubbliche da O&P

18. SISTEMI DI MONITORAGGIO RETE AZIENDALE

Per motivi di sicurezza del sistema informatico, per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, ecc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Titolare, per il tramite degli Amministratori di Sistema e nel rispetto della normativa sulla privacy, accedere direttamente a tutti gli strumenti informatici di O&P.

Periodicamente e in presenza di anomalie, gli Amministratori di Sistema effettueranno verifiche di funzionalità approfondite che potranno determinare segnalazioni ed avvisi generalizzati diretti agli Utenti della funzione organizzativa in cui è stata rilevata l'anomalia stessa e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

O&P è tenuta comunque a denunciare all'autorità giudiziaria tutti i comportamenti contrari alla legge, anche rilevati da analisi di tipo impersonale.

19. UTILIZZO DELLA FIRMA DIGITALE

La Firma Digitale deve essere utilizzata esclusivamente dal proprietario della firma.

20. SISTEMA DI VIDEOSORVEGLIANZA

Il sistema di videosorveglianza è realizzato in alcune aree specifiche (adeguatamente indicate da cartelli informativi) con finalità di sicurezza e controllo per tutelare il patrimonio di O&P contro atti vandalici, accessi non autorizzati o guasti tecnici e strutturali, comportamenti illeciti e/o fraudolenti e per agevolare gli operatori nel controllo della sicurezza delle strutture.

L'accesso alle immagini videoregistrate è permesso esclusivamente per le finalità sopra indicate agli incaricati del trattamento ed in caso di necessità agli organi preposti delle forze dell'ordine.

21. SPECIFICI DIVIETI

Di seguito sono riportati specifici divieti per gli Utenti:

a. alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
b. accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
c. accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
d. detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico o di soggetti concorrenti, pubblici o privati al fine di acquisire informazioni riservate;

e. svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
f. svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni;
g. svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
h. svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
i. distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
j. caricare programmi non provenienti da una fonte certa e autorizzata dalla Società;
k. acquistare licenze software da una fonte (rivenditore o altro) non certificata e non in grado di fornire garanzie in merito all'originalità/autenticità del software;
l. detenere supporti di memorizzazione di programmi non originali (DVD\CD\floppy);
m. installare un numero di copie di ciascun programma ottenuto in licenza superiore alle copie autorizzate dalla licenza stessa, al fine di evitare di ricadere in possibili situazioni di *underlicensing*;
n. utilizzare illegalmente password di computer, codici di accesso o informazioni simili per compiere una delle condotte sopra indicate;
o. utilizzare strumenti o apparecchiature, inclusi programmi informatici, per decriptare software o altri dati informatici;
p. distribuire il software aziendale a soggetti terzi;
q. realizzare codice software che violi copyright di terzi;
r. accedere illegalmente e duplicare banche dati.

22. PERDITA DELLE CONDIZIONI DI INCARICATO

In caso di perdita delle condizioni di Incaricato al Trattamento o di cessazione del rapporto con O&P, valgono le seguenti regole operative:

a. Le credenziali per l'accesso ai sistemi e alla posta elettronica vengono disattivate.
b. È facoltà di O&P effettuare eventuali operazioni di conservazione di e-mail di carattere professionale di Utenti non più appartenenti all'organizzazione. Le e-mail nella "Posta personale" saranno, al contrario, cancellate.

Tali attività sono effettuate dagli Amministratori di Sistema autorizzati alla gestione della posta elettronica, che potranno pertanto avere accesso, per esclusive ragioni di carattere tecnico e solo ove non sia evitabile, a dati personali conservati all'interno delle caselle di posta.

Con il dovuto anticipo, l'Utente è tenuto ad attivare il risponditore automatico per notificare ad eventuali fornitori, partner, clienti od altri soggetti interessati, l'interruzione del proprio rapporto con O&P e - se del caso - per proporre un contatto interno alternativo.

Per quanto riguarda la restituzione degli strumenti informatici di proprietà di O&P, valgono le seguenti regole operative:
a. Gli smartphone devono essere restituiti.
b. Gli altri strumenti informatici devono essere restituiti al proprio Responsabile.

23. PRESCRIZIONE RESIDUALE

Per dubbi ed incertezze, in merito a come debba avvenire il trattamento dei dati e delle informazioni personali e aziendali, nonché sulle modalità di utilizzo degli strumenti di trattamento, l'Utente può rivolgersi al proprio Responsabile per ricevere le opportune istruzioni.

24. RESPONSABILITÀ E SANZIONI

È fatto obbligo a tutti gli Utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione del presente Regolamento è perseguibile nei confronti dell'Utente, nonché con tutte le azioni civili e penali consentite.

Chiunque non rispetti il presente Regolamento potrà essere soggetto all'immediata sospensione dell'accesso agli strumenti informatici.

25. AGGIORNAMENTO E REVISIONE

Il presente Regolamento è soggetto a revisione periodica, che potrà avvenire a seguito di cambiamenti organizzativi e normativi o necessità istituzionali. Tutte le future modifiche al presente Regolamento verranno opportunamente comunicate agli Utenti e rese pubbliche sul sito internet di O&P.

Letto ed approvato il 1 giugno 2019

OSCULATI & PARTNERS SRL

ALLEGATO 1 - MODELLO ORGANIZZATIVO DI RESPONSABILITA' PRIVACY

I SOGGETTI

Titolare del trattamento

O&P, nella persona del suo legale rappresentante
1. Decidere le finalità del trattamento 2. Nominare per iscritto gli eventuali responsabili del trattamento 3. Garantire i diritti di cui all'Art. 7 all'interessato coordinandosi con i responsabili nominati 4. Delegare ai responsabili le attività che reputa possano essere svolte da tali soggetti 5. Assicurare la formazione degli incaricati relativamente alle procedure per il trattamento coordinandosi con gli eventuali responsabili nominati *6.* Definire le regole di condotta e le indicazioni da inserire nel *regolamento informatico e linee guida* 7. Provvedere all'assunzione delle misure minime di sicurezza idonee al trattamento

Responsabile interno al trattamento

Dott. CLAUDIO RATTI
IV. Provvedere all'attuazione delle procedure per adottare ed implementare le misure di sicurezza V. Relazionare alla titolare cambiamenti, pericoli e/o rischi individuati VI. Integrare nel tempo la privacy policy con le indicazioni del Garante e della titolare VII. Formulare le nomine idonee per i responsabili esterni VIII. Organizzare la formazione a tutti gli incaricati e responsabili IX. Provvedere all'analisi dei rischi e concordare insieme alla titolare eventuali implementazioni X. Verificare che incaricati abbiano accesso ai soli dati per i quali sono autorizzati XI. Provvedere alle verifiche di conformità al D. lgs. 196/03 annualmente XII. Nominare gli incaricati al momento dell'inizio del rapporto di collaborazione / lavoro

Amministratori di rete

Amministratore di rete esterno
2. Sistemista e Manutentore del sistema informatico 3. Accesso alla rete per interventi di manutenzione e implementazione con credenziali di administrator 4. Accesso alla rete per tele assistenza con VPN 5. Installazione di nuovi elementi hardware e software 6. Installazione e manutenzione software gestionale

Amministratore di rete interno
8. Assistere l'amministrazione di rete esterno in fase di aggiornamento e manutenzione software e hardware 9. Controllare l'aggiornamento delle anagrafiche hardware e/o software in coordinamento con l'amministratore di sistema esterno 10. Mantenere segrete e riservate le credenziali di administrator fornite 11. In caso di malfunzionamento degli strumenti elettronici, analizzare l'evento e, nel caso contattare l'amministratore di rete esterno e programmarne gli interventi 12. Analisi log di sistema e gestione proxy server, per garanzia di sicurezza dei dati

Responsabili esterni al trattamento

materia	soggetto	compito
Commercialista	_____	Consulente fiscalità
Consulente del lavoro	_____	Gestione documentazione rapporti di lavoro
Sicurezza	_____	Compliance D. lgs. 81/01
Medico	_____	Controlli medici come da normativa cogente
Sicurezza informatica	_____	Assistenza, manutenzione rete informatica

Incaricati del trattamento

L'elenco degli incaricati può essere visionato presso la sede della titolare.
Sono incaricati al trattamento - nominati per iscritto dal titolare al trattamento (legale rappresentante) o dal responsabile interno adeguatamente delegato, tutto il personale dipendente, i collaboratori e le figure che, per grado di integrazione con la struttura organizzativa, possono dirsi non titolari stessi dei dati.

Ogni incaricato all'atto della nomina deve:

- prendere conoscenza dell'*informativa*, del presente *Regolamento Privacy*, del *Regolamento informatico e delle linee guida* adottate dalla titolare e all'uopo consegnategli;
- chiarire gli eventuali dubbi, incertezze dovesse avere;
- sottoscrivere la *nomina*, il presente *regolamento Privacy*, il *Regolamento informatico e le linee guida.*

L'incaricato dovrà seguire le prescrizioni indicate nel presente *Regolamento Privacy,* Regolamento *Informatico e nelle Linee Guida*.

ALLEGATO 2 – DOCUMENTO SULLA RETE E PROTEZIONE DEI DATI DI O&P

RETE E PROTEZIONE DEI DATI

Presso la sede della titolare, sono conservati in versione digitale nei server di sua proprietà, ed è possibile consultarli, i documenti relativi a:

- **Hardware**
- **Software**
- **Firewall**
- **Antivirus**
- **Proxy server**
- **Procedure di back up**
- **Procedura di data restore**

In particolare:

Assistenza rete informatica

In caso di necessità, quando l'amministratore di rete interno non può risolvere la questione, le richieste di assistenza possono essere inoltrare all'amministratore di rete esterno.

I soggetti, nominati amministratore di sistema possono intervenire anche con connessione VPN.
La procedura di tele-assistenza è dettata di concerto con l'amministratore di sistema esterno.

Sito web

I siti web utilizzati e di proprietà della titolare sono:

1. O&P

Per ogni sito è stata definita una *privacy policy* pubblicata al suo interno.

IL COMPUTER

Agli incaricati preposti viene dato in uso un computer per svolgere la propria attività. Tale strumento è collegato ai server della titolare in una rete locale ed alla rete internet.
La titolare considera gli strumenti elettronici, anche non collegati alle rete suddette, messi a disposizione degli incaricati (a seconda dei casi: computer, software navigazione su Internet, e-mail) degli strumenti di lavoro da utilizzare esclusivamente per l'esecuzione delle mansioni affidate.
A tal fine, all'incaricato vengono consegnate le credenziali di autenticazione per accedere al sistema, utilizzare la rete locale, i programmi software e le cartelle a lui accessibili, nonché la rete internet e la posta elettronica.
Attraverso le linee guida e la formazione svolta, l'incaricato prende conoscenza delle cautele necessarie per mantenere riservata la propria password, per navigare in sicurezza, non compiere azioni che possano minacciare e mettere in pericolo il sistema informatico aziendale.

LA POSTA ELETTRONICA

Gli indirizzi sotto indicati sono in uso agli incaricati nominati.
Ulteriormente agli incaricati viene assegnato un indirizzo di posta elettronica secondo le modalità previste dal *regolamento informatico e linee guida* a cui si rimanda.

PROTEZIONE FISICA DEI LOCALI E DELLE ATTREZZATURE

Sistema antincendio

I sistemi antincendio sono sottoposti a revisione nei termini prescritti dalla legge, D. Lgs. 81/08.
Gli addetti preposti come squadra antincendio hanno ricevuto l'idonea preparazione.

Sistema di allarme con videosorveglianza

Il sistema di allarme è:

- perimetrale/volumetrico (all'interno della sede)
- con videosorveglianza: presso l'entrata della sede operativa della titolare sono posizionate delle telecamere per la videosorveglianza dello spazio interno al fine di evitare che terzi estranei possano raggiungere gli uffici e altri locali della sede senza essere accompagnati..

Le immagini riprese dalle telecamere e registrate attraverso software installato su elaboratore in uso all'amministratore di sistema sono visionabili da questi e dalla direzione di O&P.

Tali registrazioni vengono conservate al massimo per 24 ore e cancellate successivamente con eliminazione dei file relativi dall'elaboratore.

CONSERVAZIONE e CANCELLAZIONE DEI DATI

La titolare conserva unicamente i dati necessari per svolgere al meglio la propria attività, senza ledere i diritti degli interessati.

In merito, per i dati considerati non più utilizzabili, la titolare ha dettato le seguenti procedure di cancellazione, in base al tipo di supporto utilizzato per la loro gestione:

1- *Dati su supporto cartaceo*

ogni informazione su supporto cartaceo non necessaria deve essere resa inintelligibile (con trita carta o manualmente) e quindi smaltita nel contenitore della carta.

2- Dati digitali su supporto magnetico/digitale

Per tale ambito si fa riferimento alla Scheda informativa del 12 dicembre 2008 emessa dal Garante per la protezione dei dati personali.

I dati vengono conservati su tali supporti solo per il tempo necessario a svolgere le attività inerenti.

Nel caso in cui il dispositivo elettronico da sottoporre a smaltimento non sia più funzionante, e non siano pertanto applicabili le misure software, allo scopo di garantire l'impossibilità di recupero dei dati da parte di terzi estranei occorre procedere con modalità hardware, basate sull'uso di dispositivi di demagnetizzazione), o con la distruzione fisica.

Amministratori di rete

Sistemista e Manutentore del sistema informatico

O&P ha attivo un contratto per l'esternalizzazione del SIA ad una Azienda terza quale _____che detiene una copia di tutte le credenziali dei sistemi server con l'utilizzo dell'esclusiva manutenzione dei sistemi.

Accesso alla rete per interventi di manutenzione e implementazione con credenziali di administrator

L'azienda _____ in possesso delle credenziali di amministrazione dei sistemi ne garantisce il possesso, l'archiviazione tramite sistemi di sicurezza e la non divulgazione ad entità terze e l'utilizzo esclusivo per le attività di manutenzione

Accesso alla rete per tele assistenza con VPN

L'azienda _____ tramite il software _____ garantisce la sicurezza dei collegamenti con il tracciamento delle attività degli operatori che agiscono tramite teleassistenza.

Non esistono ad oggi collegamenti VPN in essere

Installazione di nuovi elementi hardware e software

Tutte le attività di implementazione/modifica hardware e software sono delegate all'amministratore di rete.

Installazione e manutenzione software gestionale

L'installazione e la manutenzione del software gestionale sono installate manutenute e gestiste dalla software house della *Wolter Kluwer*

Amministratori di rete interno

Ad oggi O&P ha nominato un collaboratore con la delega di amministratore di rete interna.