Incarico per il trattamento di dati personali ai sensi dell'art. 28 del Regolamento UE 2016/679 (GDPR)

Introduzione

Questo documento, che costituisce un allegato ai Termini e Condizioni del Contratto di Licenza d'Uso e Fornitura di Servizi, specifica gli obblighi delle Parti relativamente alla protezione dei dati personali.

DNR Informatica S.r.l. tratterà i dati personali per conto del Cliente ai sensi dell'Art. 4 (2) e Art. 28 del Regolamento europeo in materia di protezione dei dati personali (GDPR).

Il Cliente (Titolare del trattamento come indicato all'art. 4 (7) GDPR) è responsabile, nel quadro del presente incarico, dell'osservanza delle disposizioni di legge sulla protezione dei dati, in particolare della legalità nella comunicazione di dati alla DNR Informatica S.r.l., così come della legalità del trattamento dati.

Responsabile Esterno del Trattamento è DNR Informatica S.r.l.

I. Oggetto e durata dell'incarico

1) **Oggetto dell'incarico**
L'Oggetto del presente incarico inerisce al Contratto di Licenza d'Uso e Fornitura di Servizi in essere tra le nostre Società cui si fa qui riferimento (nel seguito: il Contratto Principale).

2) Durata dell'incarico
La durata del presente incarico sarà uguale a quella del Contratto Principale.
Sono applicabili le regole sul recesso come nel Contratto Principale.

II. Specifiche dell'incarico

1) Oggetto, tipo e scopo del trattamento o utilizzo dei dati personali
Il trattamento dei dati personali è eseguito esclusivamente per gli scopi descritti in Allegato 1.

2) Ubicazione del trattamento dati
Tutti i trattamenti di dati contrattualmente concordati avverranno in Italia o in uno Stato Membro dell'Unione Europea.

3) Tipo di dati personali
Il tipo di dati personali trattati da DNR Informatica S.r.l. è specificato nell'Allegato 2.

4) Categorie di soggetti interessati
Gli interessati dal trattamento di dati da parte di DNR Informatica S.r.l. sono specificati nell'Allegato 3.

III. Misure tecniche e organizzative

1) DNR Informatica S.r.l. documenterà le misure tecniche e organizzative concordate durante l'iter di esecuzione dell'ordine prima dell'inizio del trattamento, in particolare relativamente all'esecuzione dell'ordine specifico. Il Cliente è responsabile per la scelta di misure tecniche e organizzative idonee ed effettive. Nel caso in cui si renda

necessaria una verifica da parte dell'Autorità Responsabile della Protezione dei Dati, questa dev'essere implementata per mutuo accordo tra le Parti entro un adeguato periodo di tempo.

2) DNR Informatica S.r.l. stabilirà i requisiti di sicurezza del trattamento ai sensi dell'art. 28 (3c), e dell'art. 32 del GDPR, in particolare in collegamento con l'art. 5 del GDPR, utilizzando le misure concordate. Complessivamente, le misure da adottare sono misure sulla sicurezza dei dati e sono volte a garantire un livello di protezione appropriato al rischio, relativamente alla riservatezza, integrità, disponibilità, e resilienza del sistema. Facendo

3) questo, DNR Informatica S.r.l. terrà in considerazione lo stato dell'arte, i costi d'implementazione e il tipo, la portata e gli scopi del trattamento, come anche la probabilità e la gravita del rischio per i diritti e libertà delle persone fisiche ai sensi dell'art. 32 (1) del GDPR, come in Allegato 4.

4) Le misure tecniche e organizzative sono soggette al progresso tecnico e a ulteriore sviluppo. A questo riguardo, a DNR Informatica S.r.l. è permessa l'implementazione di adeguate misure alternative, fermo restando che il livello di sicurezza delle misure determinate non debba mai venire meno. DNR Informatica S.r.l. documenterà le modifiche, quando sostanziali.

IV. Facoltà del Cliente di impartire istruzioni

1) DNR Informatica S.r.l. tratterà tutti i dati personali esaustivamente nel quadro degli accordi fatti secondo le istruzioni dei Cliente (art. 29 GDPR), a condizione che non sia obbligato al trattamento ai sensi di Leggi UE o dello Stato; in tale caso, DNR Informatica S.r.l. informerà il Cliente di questi requisiti legali prima del trattamento, a condizione che la legge cui si fa riferimento non proibisca tale notifica sulla base di un pubblico interesse essenziale. Le istruzioni dovranno inizialmente essere definite in questo incarico, e potranno essere modificate, integrate o sostituite da parte del Cliente ai sensi di questo incarico tramite istruzioni individuali per iscritto o in formato elettronico, all'ufficio designato da DNR Informatica S.r.l., che le conserverà in una directory dedicata in forma elettronica.

2) Il Cliente dovrà sempre confermare le istruzioni verbali per iscritto oppure elettronicamente.

3) DNR Informatica S.r.l. non utilizzerà i dati personali per alcun altro scopo se non quelli concordati, in particolare non per scopi propri o quelli di terzi. Copie e duplicati non potranno essere effettuate senza che il Cliente ne sia a conoscenza. Restano escluse le copie di backup, nella misura in cui queste siano necessarie per garantire il corretto trattamento dei dati, e i dati personali che sono necessari, relativamente all'osservanza degli obblighi legali sulla loro custodia.

4) DNR Informatica S.r.l. darà notifica immediata al Cliente se valuterà che un'istruzione violi le norme sulla protezione dei dati e avrà il diritto di sospendere l'osservanza di tale istruzione fino a quando non sia confermata o modificata dal Cliente.

5) La persona che rappresenta DNR Informatica S.r.l. autorizzata a ricevere istruzioni dal Cliente è l'ing. Roberta Russo, avente facoltà di farsi assistere in tale ruolo dal personale tecnico avente in carico il Cliente.

6) Se un'istruzione richiede attività che esulino dai servizi concordati nei Contratto Principale, DNR Informatica S.r.l. può farlo presente, nonché richiedere un appropriato pagamento per eseguirla.

V. Rettifica, cancellazione e limitazioni al trattamento dei dati personali

1) Nella misura in cui un soggetto interessato specifico solleva una rivendicazione direttamente contro DNR Informatica S.r.l. per informazione, rettifica, cancellazione, limitazione del trattamento, portabilità dei dati (art. 15 GDPR), DNR Informatica S.r.l. inoltrerà immediatamente tale richiesta al Cliente. DNR Informatica S.r.l. sarà tenuta esclusivamente all'attività richiesta da parte dell'interessato.

2) Indipendentemente da quanto previsto al punto 1, DNR Informatica S.r.l., a seguito di previa comunicazione del Cliente, ha la facoltà di cancellare i dati personali se è nella misura in cui questo sia necessario per un miglior servizio come previsto nel Contratto Principale, purché al Cliente sia garantita la possibilità di avere un backup dei dati.
3) I costi sostenuti da DNR Informatica S.r.l. per tale specifica assistenza fornita al Cliente per soddisfare i diritti dell'interessato conformemente a questa Sezione V, devono essere compensati sulla base delle condizioni convenute tra le Parti nel Contratto Principale.

VI. Responsabile della protezione dei dati (DPO)

1) DNR Informatica S.r.l. non rientra tra i soggetti tenuti alla nomina del Data Protection Officer ai sensi dell'art. 37 del GDPR.

VII. Riservatezza

1) DNR Informatica S.r.l., nell'esecuzione del Contratto Principale, impiegherà solo dipendenti obbligati a mantenere la riservatezza e che sono stati resi anticipatamente edotti sulle relative disposizioni sulla protezione dei dati. DNR Informatica S.r.l., e qualsiasi persona subordinata ad essa, che abbia accesso ai dati personali, potrà trattare tali dati solo secondo le istruzioni da parte del Cliente, incluse le specifiche previste ai sensi di questo incarico.
2) ll Cliente e DNR Informatica S.r.l. sono tenuti a trattare con riservatezza tutte le conoscenze relative a segreti commerciali e le misure di sicurezza sui dati ottenuti dell'altra rispettiva Parte nell'ambito del rapporto contrattuale. Tale obbligo rimane in vigore anche dopo la conclusione del Contratto.

VIII. Obbligo d'evidenza e ispezione di DNR Informatica S.r.l.

1) DNR Informatica S.r.l. verificherà regolarmente i propri processi interni, come anche le misure tecniche e organizzative ai sensi dell'Allegato 4, onde garantire che il trattamento nella sua area di responsabilità avvenga in osservanza dei requisiti della legge applicabile alla protezione dei dati e che siano garantiti i diritti della persona interessata.
2) A DNR Informatica S.r.l. potrà essere richiesta prova delle misure tecniche e organizzative adottate su richiesta del Cliente nel contesto dei propri poteri d'ispezione ai sensi della Sezione X di questo documento.

IX. Subappalto

1) DNR Informatica S.r.l. ha facoltà di avvalersi di altro Responsabile (altri soggetti che elaborino dati, ai sensi dell'art. 28 (2), (4) GDPR).
2) Vi è un rapporto di subappalto nel caso DNR Informatica S.r.l. commissioni al sub-responsabile l'intero servizio o parte del servizio che deve contrattualmente al Cliente. DNR Informatica S.r.l. selezionerà i sub-responsabili con cura, tenendo in speciale considerazione le misure tecniche e organizzative adottate dai suddetti, e stipulerà accordi al fine di garantire l'appropriata protezione e le misure di sicurezza per le informazioni.
3) DNR Informatica S.r.l. è tenuta a informare il Cliente prima di coinvolgere eventuali sub-responsabili o di sostituire quelli esistenti. Il Cliente può obiettare a cambiamenti motivati entro 14 giorni dalla comunicazione del

cambiamento. Nel caso non siano sollevate obiezioni in tale periodo, sarà dato per inteso che tale consenso al cambiamento sia stato accordato. Se il Cliente sollevasse obiezioni al subappalto e se non fosse possibile per DNR Informatica S.r.l. nominare altro sub-responsabile a condizioni adeguate nel breve periodo, DNR Informatica S.r.l. ha il diritto, a sua discrezione, di adeguare il pagamento concordato agli ulteriori costi sostenuti per via del subappalto alternativo, o di porre termine a questo incarico e al Contratto Principale.

4) Se DNR Informatica S.r.l. emette ordini nei confronti dei sub-responsabili, trasferirà da questo incarico i propri obblighi di protezione dei dati in misura appropriata e adatta ai sensi dell'art. 28 (4) e (9) del GDPR. A questo fine, dovrà concludere un accordo scritto con il sub-responsabile e assicurare l'osservanza di tali obblighi.

5) Non sono considerati come subappalto ai sensi del presente incarico, eventuali servizi che DNR Informatica S.r.l. definisce come servizi ausiliari di supporto nella gestione delle attività. Tali servizi ausiliari includono ad es. servizi di telecomunicazione, manutenzione dei propri apparati, smaltimento di apparati e supporti dati, etc. per i quali, comunque, DNR Informatica S.r.l. adotterà tutte le misure di controllo per garantire la sicurezza dei dati.

X. Diritti di controllo del Cliente

1) Il Cliente ha il diritto, consultandosi con DNR Informatica S.r.l., di richiedere prove sull'osservanza di questo incarico da parte di DNR Informatica S.r.l., ogni due anni nella misura in cui sia necessario e ragionevole. DNR Informatica S.r.l. dovrà fornire prova sull'osservanza di questo incarico fornendo opportuna documentazione. Se tale documentazione fosse palesemente insufficiente come evidenza dell'osservanza dell'incarico, DNR Informatica S.r.l. dovrà rendere possibile al Cliente, con coordinamento congiunto, di eseguire un'ispezione in sito nella propria sede. Il Cliente assumerà qualsiasi responsabilità nel garantire che tali ispezioni siano effettuate da proprio personale opportunamente qualificato e obbligato alla riservatezza, o che le stesse siano affidate a ispettori esterni opportunamente qualificati e obbligati alla riservatezza, da nominarsi ogni singola volta. I costi che DNR Informatica S.r.l. sosterrà per questa cooperazione nelle ispezioni saranno compensati sulla base delle condizioni convenute tra le Parti nel Contratto Principale.

2) L'evidenza di tali misure, che non si riferiscono solo all'ordine specifico, può anche ottenersi con l'osservanza di codici di condotta approvati ai sensi dell'art. 40 del GDPR, con la certificazione secondo una procedura di certificazione approvata ai sensi dell'art. 42 del GDPR, con eventuali attestati o relazioni da parte di autorità indipendenti (contabili, auditor, funzionari per la protezione dei dati, dipartimenti per la sicurezza IT, auditor sulla protezione dei dati, auditor della qualità) o a seguito di un'idonea certificazione tramite audit di protezione dati.

XI. Notifica e azioni di DNR Informatica S.r.l. in caso di violazioni

1) DNR Informatica S.r.l. informerà il Cliente immediatamente se venisse a conoscenza di violazioni della sicurezza dei dati personali del Cliente o di altre violazioni delle disposizioni di legge o disposizioni del presente incarico, e adotterà opportune misure per garantire la sicurezza dei dati personali e ridurre possibili conseguenze negative per il Cliente o per gli interessati, coordinandosi con il Cliente stesso.

2) DNR Informatica S.r.l. notificherà immediatamente al Cliente eventuali attività ispettive o altre misure adottate dalle autorità di vigilanza, nella misura in cui queste si riferiscano al presente incarico. Queste disposizioni si applicano anche nel caso in cui l'autorità responsabile conduca indagini relativamente al trattamento di dati personali da parte di DNR Informatica S.r.l. per conto del Cliente, nel quadro di illeciti amministrativi o procedimenti penali. Il Cliente e DNR Informatica S.r.l. coopereranno per ottemperare alle richieste nei confronti delle autorità di vigilanza.

3) Il Cliente, a sua volta, può essere soggetto ad ispezioni delle autorità di vigilanza su illeciti amministrativi o procedimenti penali, rivendicazioni di responsabilità da parte di interessati o di terzi, oppure di altre rivendicazioni relative al trattamento dei dati nell'ambito di quanto oggetto del presente incarico. DNR Informatica S.r.l. collaborerà con il Cliente nell'esercizio della protezione legale contro tali misure o per difendersi contro tali

rivendicazioni al meglio dei suoi poteri e nella misura necessaria e ragionevole. I costi che DNR Informatica S.r.l. sosterrà per tale collaborazione saranno compensati sulla base delle condizioni convenute tra le Parti nel Contratto Principale.
Le disposizioni di cui sopra sono valide e non cambieranno anche dopo la conclusione del presente incarico fino a quando gli obblighi disposti in esso saranno soddisfatti appieno.

XII. Cancellazione e restituzione dei dati personali

1) DNR Informatica S.r.l. è tenuta a restituire qualsiasi documentazione di cui sia venuta in possesso. Tutti i dati risultanti dal trattamento e utilizzo e tutti i dati raccolti relativamente all'incarico da parte del Cliente saranno distrutti, in ottemperanza agli standard sulla sicurezza informatica, entro sei mesi dalla cessazione del Contratto Principale o anche prima, su richiesta del Cliente, a condizione che non vi siano legittimi interessi di DNR Informatica S.r.l. in contrasto con tale mandato. La disposizione di cui sopra non si applica in particolare se la cancellazione non sia tecnicamente possibile o si configuri con costi sproporzionati per DNR Informatica S.r.l.
2) DNR Informatica S.r.l. può conservare documentazione che comprovi l'appropriato trattamento dei dati secondo l'incarico ricevuto o che possa servire come protezione legale dopo la conclusione del Contratto Principale per i periodi di ritenzione stabiliti per legge o concordati per contratto.

XIII. Ulteriori compiti di DNR Informatica S.r.l.

DNR Informatica S.r.l. è disponibile nel supportare il Cliente e a cooperare con esso in misura necessaria e ragionevole, su specifica richiesta:

a. nel quadro relativo alla salvaguardia dei diritti degli interessati, ai sensi dell'art. 12 del GDPR;
b. per la valutazione sull'impatto della protezione dei dati, ai sensi dell'art. 35 del GDPR;
c. nel quadro relativo a precedenti consultazioni con le autorità di sorveglianza, ai sensi dell'art. 36 del GDPR, anche con l'accesso al proprio registro delle attività di trattamento, ai sensi dell'art. 30 del GDPR, per rendere disponibili le necessarie informazioni al Cliente.

XIV. Disposizioni finali

1) È richiesta la forma scritta per qualsiasi modifica al presente incarico.
2) Se parti individuali del presente incarico risultassero non valide, ciò non inficerà la validità delle rimanenti disposizioni del Contratto.

_____

Luogo / data Timbro e firma Cliente

Sant'Agnello, 11/07/2018 _____

data DNR Informatica S.r.l.

Allegato 1

Oggetto del trattamento

DNR Informatica S.r.l. accede in modalità remota ai sistemi del Cliente esclusivamente per finalità di manutenzione e/o aggiornamento dei propri software.
DNR Informatica S.r.l. non effettua alcuna interazione, modifica e/o aggiornamento di sistemi operativi né di qualsiasi altra applicazione presente sui sistemi su cui è installato il proprio software, utilizzata dal Cliente per le proprie attività, per cui in nessun caso potrà essere accettato il ruolo di amministratore di sistema per conto del Cliente.
DNR Informatica S.r.l., nell'esercizio delle proprie attività, può accedere in maniera occasionale a dati personali gestiti dall'applicazione, il trattamento dei quali ricade sotto le vigenti disposizioni di legge per la protezione dei dati.

Allegato 2

Tipo di Dati Personali trattati

DNR Informatica S.r.l. potrà venire occasionalmente a conoscenza nel corso delle proprie attività, comunque non finalizzate al trattamento di dati personali, delle seguenti tipologie di dati presenti negli applicativi del Cliente:

- Anagrafica delle persone (cognome, nome, …);
- Dati contabili e amministrativi (fatturazione, contratti, pagamenti, …);
- Dati relativi alla gestione del personale (rapporti di lavoro, cedolini paga, certificazioni, …);
- Dati relativi alla gestione dell'ospitalità alberghiera (date del soggiorno, numero e tipologia di camera, ragione sociale, carte di credito, …);
- Altre informazioni da input in campi liberi che potrebbero essere utilizzati dal Cliente anche per l'inserimento di dati sensibili.

Allegato 3

Categorie di soggetti interessati

DNR Informatica S.r.l. potrà venire occasionalmente a conoscenza nel corso delle proprie attività, comunque non finalizzate al trattamento di dati personali, di dati personali relativi alle seguenti categorie di soggetti interessati, presenti negli applicativi del Cliente:

- Ospiti della struttura del Cliente;
- Personale dipendente del Cliente;
- Dipendenti di terzi e consulenti che prestano servizi al Cliente;
- Clienti/fornitori del Cliente.

Allegato 4

Misure di sicurezza tecniche e organizzative

1. Riservatezza (Articolo 32 (1b) GDPR)

1.1. Controllo ingressi

Le seguenti misure evitano l'ingresso a persone non autorizzate all'interno dei locali che ospitano i sistemi di elaborazione dati con i quali i dati personali vengono elaborati o utilizzati

- Procedura vincolante per l'assegnazione e l'invio di autorizzazioni all'ingresso degli uffici.
- Gestione controllata delle chiavi.
- Politica per l'accompagnamento dei visitatori.
- Chiusura a chiave di armadi e uffici durante il periodo di assenza del personale.

1.2. Controllo di ammissione

Misure per impedire l'utilizzo dei sistemi di elaborazione dati da parte di personale non autorizzato:

- Ammissione solo dopo identificazione e autenticazione.
- Procedura vincolante per l'assegnazione delle autorizzazioni di ammissione.
- Assegnazione univoca di account utenti.
- Politica per un utilizzo sicuro e appropriato delle password.
- Blocco automatico dell'account utente dopo un certo numero di tentativi di login falliti o dopo un certo periodo di inattività.
- Blocco automatico dei computer dopo un cerio periodo di inattività con conseguente ripetizione del login.
- Standby automatico dei computer locali.
- Registrazione accessi e analisi dei file di log.
- Cancellazione controllata dei dati personali dopo la scadenza del contratto.

1.3. Controllo accessi

Misure per assicurare che le persone autorizzate all'utilizzo dei sistemi di elaborazione dati abbiano accesso solo ai dati conformi alla loro autorizzazione tramite login, e che i dati personali non possano essere Ietti, copiati, modificati o rimossi in modo non autorizzato durante l'elaborazione:

- Concetto di autorizzazione e ruolo organizzati.
- Procedura vincolante per l'assegnazione delle autorizzazioni di accesso.
- Revisione regolare delle autorizzazioni esistenti.
- Concetto di cartelle differenziate (convenzione di denominazione chiara per i file).
- Personalizzazione delle impostazioni di default rilevanti per la sicurezza su nuovi sistemi e applicazioni IT e disattivazione di programmi e funzioni rilevanti per la sicurezza, non necessari.
- Etichettatura chiara e conservazione sicura dei supporti dati.
- Cancellazione sicura dei dati.
- Politica "scrivania pulita/schermo pulito".
- Archiviazione dati ad accesso protetto.

1.4. Controllo della separazione

Misure per assicurare che i dati raccolti per scopi diversi vengano elaborati separatamente:

- Separazione logica attraverso regole di accesso.
- Accesso alle registrazioni solo attraverso applicazioni che soddisfino i requisiti di separazione.
- Separazione dei sistemi di produzione e test.

1.5. Anonimizzazione

Misure per assicurare che non possa essere prodotto alcun riferimento personale ai dati:

- Sono possibili analisi nelle applicazioni “per default" senza riferimenti personali.
- Possibilità di valutazione anonima da parte del Cliente.
- Dati personali sensibili conservati in forma crittografata, in conformità con le norme di sicurezza in vigore.

2. Integrità (Articolo 32 (1b) GDPR)

2.1. Controllo trasferimenti

Misure per assicurare che i dati personali non possano essere letti, copiati, modificati o rimossi da persone non autorizzate durante il trasferimento elettronico, durante il trasporto o durante il salvataggio su supporti dati, e che possano essere effettuate verifiche e presentate prove per quanto riguarda i frangenti in cui vengono pianificati i trasferimenti di dati personali con l’utilizzo di attrezzature di trasferimento dati:

- Comunicazione crittografata su reti non sicure basata sui comuni standard di sicurezza.
- Smaltimento dei supporti dati non più necessari.
- Opzione della firma elettronica nelle comunicazioni email personali.
- Divieto di utilizzo di hardware e software non autorizzati.
- Nessun inoltro di informazioni a servizi IT esterni non validati (indirizzi e-mail privati, salvataggio su cloud non autorizzati, …).
- Indicazioni specifiche ai dipendenti sulla stampa di documenti sensibili e indicazioni specifiche ai dipendenti sull’utilizzo di supporti dati.

2.2. Controllo dei dati in ingresso

Misure per assicurare una revisione successiva e verifica se i dati personali siano stati inseriti, modificati o rimossi dai sistemi di elaborazione dati, e se sì, quali:

- Accesso ai sistemi di elaborazione dati possibile solo dopo il login.
- Nessuna divulgazione delle password (politica delle password).
- Politica che definisce le procedure da seguire nel caso in cui una password diventi nota (politica delle password).

3. Disponibilità e capacità (Articolo 32(1b) GDPR)

3.1. Controllo disponibilità

Misure per assicurare che i dati personali siano disponibili e protetti da distruzioni o perdite accidentali:

- Concetto di backup e recupero documentati, con backup regolare e salvataggio a prova di disastro dei supporti dati.
- Uso di controlli dl sicurezza come ad esempio sistemi di archiviazione protetti da virus e tramite firewall ridondanti.
- Archiviazione separate dei dati.
- Protezione da incendi, surriscaldamenti, danni da acqua, picchi di tensione e perdite di potenza nel locale dei server.
- Uso di UPS e generatori di emergenza.
- Concetto di emergenza in loco (incluse verifiche regolari di efficacia).
- Monitoraggio del sistema per rilevamento guasti.

4. Procedure per la revisione, verifica e valutazione periodica (Articolo 32 (1d) del GDPR; Articolo 25 (1) del GDPR)

4.1. Gestione della privacy

Misure per assicurare che i passaggi tecnici e organizzativi effettuati restino efficaci in modo permanente:

- Controllo regolare dei passaggi tecnici e organizzativi effettuati.
- Valutazione di messaggi e report su incidenti insoliti.
- Addestramento del personale alla gestione dei rapporti con il servizio IT per aumentare la consapevolezza sulla sicurezza informatica.
- Addestramento professionale regolare del personale.

5. Misure di sicurezza implementate nei software

Tali misure devono essere correttamente impostate da parte del Cliente

- User name: l'accesso al sistema avviene solo attraverso l'identificazione univoca del soggetto che vi accede. Il Cliente deve avere adottato una procedura organizzativa affinché ogni utenza sia assegnata ad un unico addetto al trattamento di dati personali e sia gestita in conformità alle buone regole di gestione. Questa user name non potrà mai essere comunicata a chi non è stato formalmente incaricato a tale fine.
- Password: le regole di costruzione della password sono configurabili nel sistema da parte del Cliente, che potrà scegliere tra diversi gradi di complessità e applicarli a tutti gli utenti del sistema. Sono configurabili anche i tempi di sostituzione delle password.
- Disattivazione delle credenziali: esiste la possibilità di cancellazione delle credenziali inutilizzate da parte del Cliente.
- Attivazione del profilo utente. Sarà il Cliente, in autonomia, a scegliere la profilazione utente idonea e ad attribuire le autorizzazioni in funzione dell'area di cui fa parte l'utente o del profilo di autorizzazione individuale.

6. Misure di sicurezza implementate per i servizi di assistenza

6.1. Assistenza on site

- Gli addetti accedono presso la struttura del Cliente per effettuare attività tecnica di manutenzione o fare formazione. Nel caso dell'assistenza on site gli addetti lavorano come se facessero parte della struttura del Cliente, e sono tenuti ad adottare tutte le procedure di sicurezze implementate dal Cliente stesso. I Clienti, a loro discrezione, potranno generare utenze individuali per l'accesso degli addetti ai loro sistemi, oppure potranno far accedere in affiancamento, sotto il controllo del loro personale.
- Qualora durante l'attività di assistenza l'addetto abbia la necessità di prelevare dati e/o archivi di cui necessita per risolvere le problematiche evidenziate, ne chiederà l'autorizzazione al Cliente e registrerà tale evenienza nel rapporto d'intervento. Al termine dell'attività presso gli uffici, si provvederà alla immediata cancellazione totale dei dati e/o archivi.

6.2. Assistenza telefonica

- La comunicazione è esclusivamente verbale, per cui tale forma di assistenza non presenta alcuna criticità dal punto di vista del trattamento di dati personali, in quanto non è possibile alcun tipo di accesso a dati personali, né sono trasmessi dati e/o archivi.

6.3. Assistenza remota tramite collegamento Live Care

Questa modalità di collegamento al sistema del Cliente è sicuramente in grado di garantire la sicurezza dei dati personali in quanto:

- Il collegamento è sempre richiesto e attivato dal Cliente.
- Le credenziali di accesso sono sempre individuali.
- Il Cliente ha la facoltà di monitorare l'attività effettuata da remoto e di disconnettere l'addetto in qualsiasi momento.
- Solo in casi particolari, dopo attenta valutazione e con l'autorizzazione del Cliente, si può decidere di utilizzare altri strumenti di connessione equivalenti e che garantiscano gli stessi standard di sicurezza.

6.4. Trasferimento e condivisione di file in modalità FTP

- L'area FTP è configurata in modo che il Cliente possa accedere solo a propri files, caricati in upload e/o disponibili per il download. Sette giorni dopo la data di pubblicazione una routine cancella i file caricati in area FTP. I files ricevuti sono trasferiti in una directory gestita dal gruppo di assistenza, non soggetta a backup, da cui saranno rimossi al termine delle attività.
- L'archivio ricevuto in nessun caso sarà visibile a gruppi di lavoro non direttamente coinvolti nelle attività finalizzate alla risoluzione del problema segnalato dal Cliente.