PRIVACY BY DESIGN

REDATTO AI SENSI DEL D.LGS. 196/2003, COME MODIFICATO DAL D.LGS. 101/2018 E REGOLAMENTO EUROPEO 679/2016

****

PREMESSA

Il presente documento è stato redatto in conformità a quanto previsto dalla normativa nazionale in vigore, ed in particolare in conformità a quanto statuito dal D.lgs. n. 196/2003 "Codice in materia di protezione dei dati personali", come modificato dal D.lgs. 101/2018 nonché ai sensi del Regolamento Europeo 679/2016 in materia di protezione dei dati personali, ed è suddiviso come segue.

INDICE

1. SCOPO E CAMPO DI APPLICAZIONE

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il *titolare del trattamento* ha inteso di mettere in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie

garanzie al fine di soddisfare i requisiti del Europeo n. 679/2016 e tutelare i diritti degli interessati (art. 25.1 Regolamento Ue 679/2016).

Obiettivi del presente documento risultano dunque:

(i) illustrare i luoghi in cui vengono trattati i dati personali, i soggetti coinvolti nel trattamento dei dati personali, e gli strumenti utilizzati per il trattamento dei dati personali;
(ii) illustrare le finalità del trattamento cui sono destinati i dati personali, la base giuridica del trattamento, le categorie di destinatari dei dati personali, il periodo di conservazione dei dati personali;
(iii) illustrare le misure di sicurezza organizzative, fisiche e logiche che il *titolare del trattamento* attua al fine di garantire che il trattamento dei dati personali si svolga in maniera lecita, nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'Interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali;
(iv) definire sotto il profilo normativo gli obblighi che il *titolare del trattamento* deve adempiere in merito all'adozione delle misure di sicurezza;
(v) tutelare gli interessi dei soggetti privati e pubblici che fanno affidamento sui trattamenti svolti dal *titolare del trattamento*;
(vi) evitare eventi pregiudizievoli che possono danneggiare disponibilità, riservatezza e integrità del patrimonio dei dati del *titolare del trattamento*;
(vii) potenziare la consapevolezza dei rischi e delle insidie che possono coinvolgere la gestione e l'utilizzo dei sistemi informativi automatizzati ed anche l'archivio cartaceo;
(viii) definire le migliori soluzioni tecniche e/o organizzative al fine di prevenire situazioni di pericolo;
(ix) individuare le misure di sicurezza e le procedure per ridurre al minimo, la distruzione e la perdita dei dati, la modifica o la divulgazione non autorizzata, l'accesso non autorizzato, e il trattamento non consentito o non conforme.

Il *titolare del trattamento* ha definito di mettere in atto misure di sicurezza indicate nel presente documento per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. (art. 25.2 Regolamento Europeo n. 679/2016).

2. LUOGHI IN CUI VENGONO TRATTATI I DATI PERSONALI

Il trattamento avviene presso la sede operativa in viale Divisione Garibaldi n. 12 – 52037 Sansepolcro (Ar), nonché presso i responsabili indicati nel presente documento.

3. SOGGETTI COINVOLTI NEL TRATTAMENTO DEI DATI PERSONALI

3.1 TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

Descrizione	Nomine e documenti
La persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali (art. 4 co. 1 n. 7 Regolamento Europeo 679/2016)	Il *titolare del trattamento* è White Label S.r.l., p.iva 03401510544, con sede legale in Via Merlino Pazzaglia n. 7 – 06012 Città di Castello (Pg)

3.2 RESPONSABILE PER LA PROTEZIONE DEI DATI (DPO)

Descrizione	Nomine e documenti
La persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento (considerando n. 97 Regolamento Europeo 679/2016)	Il Responsabile per la protezione dei dati (DPO) è l'Avv. Edoardo Stoppa, p.iva 02155290519, con studio in via XXV aprile n. 62 – 52037 Sansepolcro (Ar). Lo stesso ha ricevuto dal *titolare del trattamento* una

	lettera controfirmata per accettazione e allegata al presente documento

3.3 AMMINISTRATORE DI SISTEMA INFORMATIVO AZIEDALE

Descrizione	Nomine e documenti
Figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (art. 32 Reg. Ue 679/2016; Provvedimento del Garante del 27 novembre 2008)	L'amministratore di sistema ha ricevuto dal *titolare del trattamento* una lettera riportante compiti e responsabilità. Tale lettera è controfirmata per accettazione e allegata al presente documento

3.4 RESPONSABILE ESTERNO AL TRATTAMENTO DEI DATI PERSONALI

Descrizione	Nomine e documenti
Persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 28 Regolamento Europeo 679/2016)	Ogni responsabile esterno per il trattamento dei dati personali ha ricevuto dal *titolare del trattamento* una lettera riportante compiti e responsabilità. Tali lettere sono controfirmate per accettazione e allegate al presente documento La nomina di incarico di responsabile esterno per il trattamento dei dati personali verso società di provider di posta elettronica e provider di servizi web, risulta da contratto in forma scritta a far data dall'aperura del servizio.

3.5 INCARICATO AL TRATTAMENTO DEI DATI PERSONALI

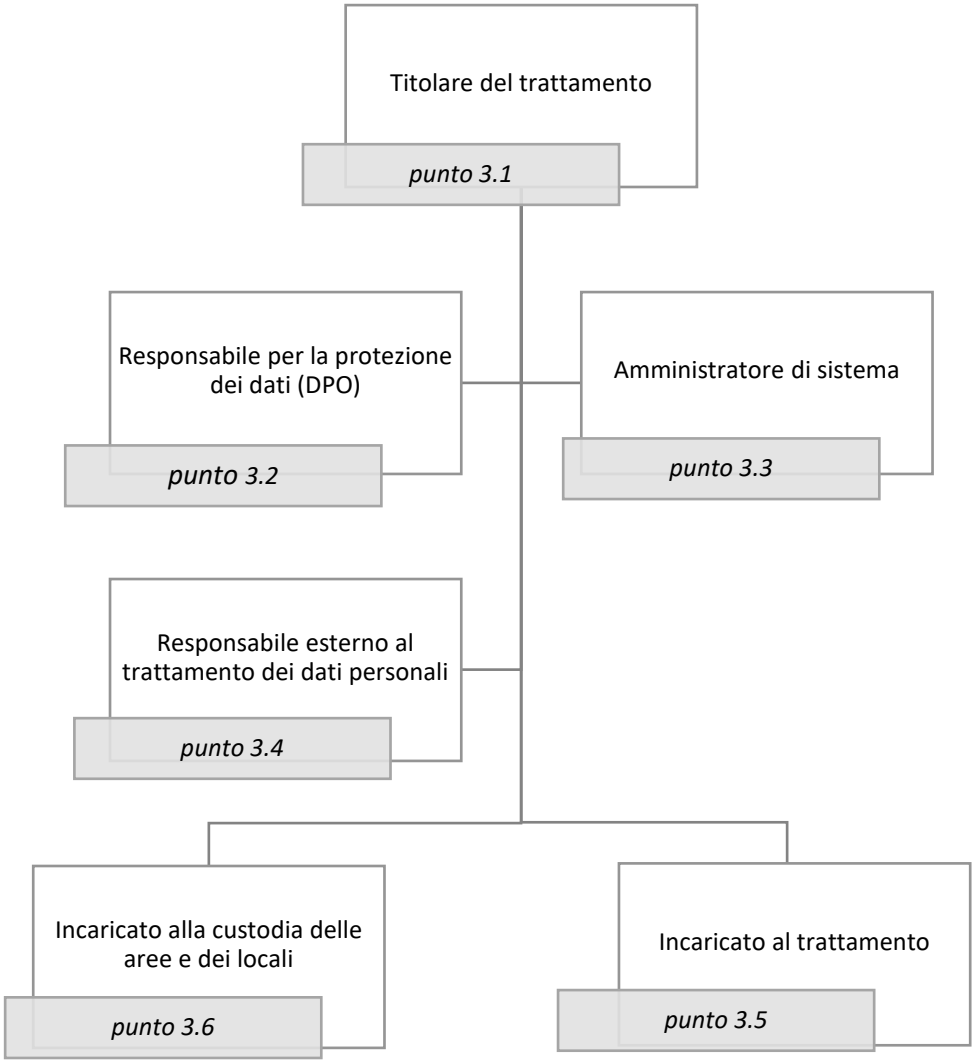
Descrizione	Nomine e documenti
Le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile e che, seppur a diversi livelli, possono effettuare operazioni di trattamento dei dati (art. 4 co. 1 n. 10 Regolamento Europeo 679/2016)	Ogni persona autorizzata al trattamento dei dati ha ricevuto dal *titolare del trattamento* una lettera riportante compiti e responsabilità. Tali lettere sono controfirmate per accettazione

3.6 INCARICHI ORGANIZZATIVI

Descrizione	Nomine e documenti
L'incaricato alla custodia delle aree, dei locali e degli archivi cartacei contenenti dati personali ha il compito di consentire l'accesso alle aree, ai locali, agli archivi cartacei, solo agli incaricati del trattamento autorizzati; controllare la chiusura dei locali, delle aree e degli archivi cartacei contente dati personali; identificare e, se del caso, registrare le persone ammesse, a qualunque titolo dopo l'orario di chiusura;	La nomina di uno o più incaricati della custodia delle copie delle credenziali è effettuata con una lettera riportante compiti e responsabilità. Tali lettere sono controfirmate per accettazione

4. ORGANIGRAMMA

In considerazione dei soggetti coinvolti nel trattamento dei dati così come specificato al precedente Punto 3, la struttura aziendale è composta come riportato nel presente organigramma.



5. FINALITÀ DI TRATTAMENTO E TIPOLOGIA DI DATI

5.1 DATI COMUNI

Finalità	Base giuridica	Interessati
Esecuzione del contratto	Adempimento del contratto e obblighi di legge ex art. 6 c. 1 lett. b) e c) Regolamento Europeo 679/2016	Fornitori, soci, clienti, collaboratori esterni e dipendenti
Tutela del patrimonio e delle frodi	Legittimo interesse del titolare ex art. 6 c. 1 lett. f) Regolamento Europeo 679/2016	Fornitori, soci, clienti, collaboratori esterni e dipendenti
Marketing diretto	Consenso espresso dell'interessato ex art. 6 c. 1 lett. a) Regolamento Europeo 679/2016	Clienti

Ricerca e selezione del personale, obblighi precontrattuali, corrispondenza	art. 111 bis D.lgs. n. 196/2003	Candidati
Cookie tecnici, analitici e di profilazione	art. 122 D.lgs. n. 196/2003 e provvedimento n. 229 dell´8 maggio 2014	Utenti sito web

5.2 DATI SEMI-SENSIBILI

Finalità	Base giuridica	Interessati
Esecuzione del contratto	Adempimento del contratto e obblighi di legge ex art. 6 c. 1 lett. b) e c) Regolamento Europeo 679/2016	Fornitori, soci, collaboratori esterni e dipendenti
Tutela del patrimonio e delle frodi	Legittimo interesse del titolare ex art. 6 c. 1 lett. f) Regolamento Europeo 679/2016	Fornitori, clienti, soci, collaboratori esterni e dipendenti

5.3 DATI PARTICOLARI

Finalità	Base giuridica	Interessati
Gestione contratti (appartenenza sindacale, dati sanitari ex Legge 104/1992)	Adempimento del contratto e consenso espresso dell'Interessato art. 9 c. 2 lett. a) Regolamento Europeo 679/2016	Dipendenti

Il *titolare del trattamento*, tenuto conto delle suddette finalità, fornisce agli interessati, al momento in cui i dati personali sono ottenuti, le informazioni di cui all'art. 13 Reg. Regolamento Ue 679/2016. Le informative sono allegate al presente documento.

6. DESCRIZIONE DEGLI STRUMENTI UTILIZZATI PER IL TRATTAMENTO

6.1 SCHEDARI E ALTRI SUPPORTI CARTACEI

I supporti cartacei e/o archivi contenenti dati personali comuni e semi-sensibili, presenti nella suddetta sede sono conservati dal *titolare del trattamento* in apposite cartelle archiviate presso l'ufficio amministrazione.

6.2 STRUMENTI ELETTRONICI

Gli strumenti elettronici contenenti dati personali comuni e semi-sensibili, presenti nella suddetta sede sono conservati dal *titolare del trattamento* nei seguenti dispositivi presso l'ufficio amministrazione.

	Dispositivo	Sistema operativo	Antivirus	Firewall	Antispam
n. 1	Pc-1	Windows Server 2012	sì	sì	sì

Il suddetto dispositivo Pc è autorizzato ad accedere alle seguenti banche dati:

(i) Gestionale Danea Easyfatt Enterprise
(ii) Servizio di posta elettronica ordinaria e certificata
(iii) Servizio Cloud

	Dispositivo	Sistema operativo	Antivirus	Firewall	Antispam
n. 1	Pc-2	Windows 10	sì	sì	sì

Il suddetto dispositivo Pc è autorizzato ad accedere alle seguenti banche dati:

(i) *Gestionale* Danea Easyfatt Enterprise
(ii) Servizio di posta elettronica ordinaria e certificata
(iii) Servizio Cloud

	Dispositivo
n. 1	Stampante laser

La suddetta unità periferica è autorizzata ad accedere ai Pc 1 e 2

6.3 STRUMENTI BACK-UP

Al fine di garantire la ridondanza dei dati contenuti negli strumenti elettronici il *titolare del trattamento* utilizza i seguenti dispositivi/servizi back-up:

	Dispositivo	Sistema operativo	Back-up
n. 1	Network Attached Storage	Windows Server 2012	Ogni 24

	Sevizio	Provider	Back-up
n. 1	Cloud One Drive	Microsoft	Tempo reale

7. PROTEZIONE DEI DATI DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA

7.1 SICUREZZA DEL TRATTAMENTO

Il *titolare del trattamento* ha progettato, per impostazione predefinita, la propria struttura al fine di prevenire la sottrazione o dispersione dei dati personali. In particolare, per massimizzare la protezione dei dati personali contenuti in schedari, supporti cartacei o elaboratori, tenuto conto dei costi di attuazione, delle finalità di trattamento, dei rischi per i diritti degli interessati, il *titolare del trattamento* ha predisposto le seguenti misure di sicurezza, organizzative, fisiche e logiche:

(i) le porte degli uffici sono chiuse nei momenti di pausa;
(ii) all'interno degli uffici è vietato fumare;
(iii) gli impianti elettrici sono a norma;
(iv) l'accesso ai locali avviene in maniera selezionata;
(v) gli schedari e altri supporti cartacei sono custoditi in stanza dedicata;
(vi) nel caso in cui dovessero essere ricevuti terzi non autorizzati, i documenti cartacei eventualmente visibili sono riposti all'interno di archivi chiusi;
(vii) i dispositivi elettronici sono protetti dal rischio d'intrusione e di virus mediante firewall e antivirus;
(viii) le banche dati contenute nei dispositivi elettronici sono dotate di parola chiave associata di accesso;
(ix) i dati contenuti nei dispositivi elettronici sono oggetto di copie di back-up;
(x) è garantita la qualità delle copie di back-up e la loro conservazione in luogo adatto e sicuro;
(xi) il servizio di posta elettronica è dotato di sistema antispam;
(xii) le misure di sicurezza sono periodicamente verificate e aggiornate mediante l'utilizzo degli strumenti più idonei per la tutela dei dati trattati;
(xiii) i dispositivi elettronici non più utilizzati sono smaltiti previa cancellazione dei dati personali ivi contenuti;
(xiv) qualora si rendesse necessario l'uso di nuovi dispositivi elettronici, sarà stabilito quali protezioni software/hardware adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato;
(xv) è previsto un sistema di videosorveglianza esterno ai locali aziendali;
(xvi) i dati trattati, scaduto il termine di conservazione, vengono distrutti;
(xvii) gli interessati vengono prontamente avvisati qualora si verifichino situazioni anomale o emergenze;

7.2 INTERVENTI E FORMAZIONE DEGLI INCARICATI

Il *titolare del trattamento* ha individuato gli incaricati al trattamento dei dati personali secondo profili di autorizzazione. Tali figure, istruite con opportune procedure operative ed incontri formativi in maniera da renderle edotte sulle metodologie di trattamento e protezione dei dati, si impegnano a garantire che le misure di sicurezza riguardanti i dati personali siano applicate all'interno dell'organizzazione aziendale ed eventualmente al di fuori,

qualora siano cedute a terzi, quali responsabili del trattamento, tutte o parte delle attività di trattamento, e ad informare il *titolare del trattamento* nella eventualità che si siano rilevati rischi.
Agli incaricati al trattamento vengono fornite esplicite istruzioni in merito ai seguenti punti:

(i) procedure da seguire per la classificazione dei dati personali;
(ii) modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia degli stessi e la loro archiviazione;
(iii) modalità per elaborare e costudire le password necessarie per accedere agli strumenti elettronici ed ai dati personali ivi contenuti;
(iv) prescrizioni per non lasciare incustoditi e accessibili gli strumenti elettronici mentre è in corso una sessione di lavoro;
(v) modalità di cancellazione dei dati personali laddove la conservazione degli stessi non sia più necessaria;
(vi) dovere di aggiornarsi utilizzando il materiale e gli strumenti forniti dal *titolare del trattamento* o dal Responsabile per la Protezione dei Dati, sulle misure di sicurezza e sulle procedure generali per il trattamento dei dati

Periodicamente si procede ad aggiornare, se necessario, la definizione dei dati cui le persone sono autorizzate ad accedere e dei trattamenti che sono autorizzate a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

8. VALUTAZIONE DI IMPATTO E ANALISI DEI RISCHI NEL TRATTAMENTO DEI DATI

8.1 CRITERI PER LA VALUTAZIONE DEL RISCHIO

La valutazione dei rischi è effettuata su tutti i processi utilizzando il seguente criterio: rischio = probabilità x danno. Dalla valutazione dei rischi deriva il carattere di urgenza o di priorità con cui intervenire sul singolo rischio. La probabilità dell'accadimento viene definita mediante la scala seguente:

Valore	Probabilità	Definizioni/criteri
1	Improbabile	Il danno può essere provocato solo indirettamente Non sono noti episodi già verificatisi
2	Poco probabile	Il danno può essere provocato solo in circostanze sfortunate. Sono noti solo rarissimi episodi già verificatisi Il verificarsi del danno susciterebbe grande sorpresa e incredulità
3	Probabile	L'inadempienza rilevata può provocate un danno anche se in modo non automatico e diretto È noto qualche episodio già verificato In verificarsi del danno susciterebbe sorpresa
4	Molto Probabile	Esiste correlazione diretta tra inadempienza rilevata e verificarsi del danno Si sono già verificati danni per la stessa inadempienza Il verificarsi del danno non susciterebbe alcuna sorpresa

Per la determinazione del livello di gravità del danno si è utilizzata la scala seguente:

Valore	Danno	Definizioni/criteri
1	Lieve	Nessuno o minimi costi per il superamento del danno Completamento solo parziale di registrazioni e/o registrazioni effettuate a posteriori oltre il momento stabilito Nessun/lieve danno all'immagine aziendale Nessuna/lieve sanzione
2	Medio	Costi per il superamento del danno

		Azioni contrarie al metodo aziendale e/o alle procedure non deliberatamente attuate Mancata registrazione dei controlli Medio danno all'immagine aziendale Sanzione di carattere medio
3	Grave	Elevati costi per il superamento del danno Azioni volutamente contrarie al metodo aziendale e/o alle procedure Non effettuazione dei controlli Mancata richiesta di autorizzazioni necessarie Danni all'immagine aziendale Sanzioni di carattere grave
4	Gravissimo	Perdita di un cliente Ingenti costi per il superamento del danno Azioni di sabotaggio al metodo aziendale e/o alle procedure Danni ingenti all'immagine aziendale Reiterata mancanza di effettuazione di controlli Sanzioni Gravissime Azioni contro la legge o norme o regolamenti Azioni contro la deontologia professionale

Il prodotto calcolato (rischio = probabilità x danno) definisce il grado di rischio ovvero la criticità dell'anomalia e permette di stabilire una gerarchia dei rischi così classificata:

Grado di rischio	Valutazione rischio	Azione corrispondente
<2	Non significativo	Nessuna azione
2-4	Basso	Le eventuali azioni da programmare sono solo per migliorare una situazione di partenza di per sé non significativamente pericolosa Introduzione di miglioramenti entro l'anno
5-8	Medio	Introduzioni di azioni correttive o migliorative da programmare entro un mese
9-16	Alto	Introduzioni di azioni correttive da programmare entro una settimana

8.2 FATTORI DI RISCHIO

Sono stati individuati i seguenti fattori di rischio che possono portare a rischi sul trattamento dei dati. L'analisi dei fattori di rischio, che dipende dalla tipologia di dati trattati, è realizzata combinando il fattore della loro l'appetibilità per terzi, con quello che esprime la pericolosità per la *privacy* dei soggetti cui essi si riferiscono.

COD	Fattori di rischio	Effetto
01	Accessi non autorizzati alle informazioni elettroniche da parte di personale interno	Integrità e riservatezza Sistemi Informativi e Gestionali
02	Accessi non autorizzati alle informazioni elettroniche da parte di personale esterno	Integrità e riservatezza Sistemi Informativi
03	Possibilità di visionare dagli schermi degli operatori le informazioni fornite dai gestionali e possibilità di intercettare le informazioni tra i terminali	Riservatezza delle postazioni locali di accesso ai gestionali
04	Furto di informazioni nei sistemi gestionali e nelle cartelle su server	Disponibilità, integrità e riservatezza delle banche dati informatiche e dei sistemi gestionali
05	Errato utilizzo dei software con pericolo di perdita delle informazioni contenute nei sistemi gestionali	Integrità dei dati contenuti nei sistemi informatici

06	Guasto di componenti hardware idonei ad interrompere la disponibilità delle informazioni	Efficienza delle infrastrutture informatiche deputate al trattamento
07	Azioni da virus o malware su sistemi di gestione e su client	Riservatezza, integrità, e disponibilità delle banche dati informatiche
08	Possibilità di conoscenza delle informazioni da parte di tecnici esterni incaricati della manutenzione delle attrezzature informatiche	Riservatezza delle banche dati informatiche
09	Perdita dei dati dovuta ad errori logici, procedurali o fisici relativi all'infrastruttura informatica	Integrità, disponibilità dei trattamenti informatici
10	Smarrimento della documentazione cartacea durante le operazioni di trattamento dei dati comuni	Disponibilità degli archivi cartacei
11	Smarrimento della documentazione cartacea durante le operazioni di trattamento dei dati relativi allo stato di salute	Disponibilità degli archivi cartacei
12	Possibilità di incendio	Integrità dei documenti
13	Situazioni che permettono la visione del contenuto dei documenti cartacei da parte di personale non autorizzato interno od esterno	Riservatezza dei documenti cartacei
14	Accesso non autorizzato dovuto a mancanza di definizione dei ruoli aziendali e di legge	Riservatezza dei dati cartacei
15	Furto di documentazione cartacea e dispositivi fisici di archiviazione dei dati informatici	Riservatezza, integrità e disponibilità
16	Errore degli operatori durante le operazioni di trattamento	Integrità e disponibilità dei dati
17	Impossibilità di accesso alle banche dati	Disponibilità dei dati

8.3 MISURE ADOTTATE

Nella valutazione dei rischi per come sopra dettagliata, sono state individuate le seguenti misure applicabili:

COD	Misura	Descrizione	Tipo
01	Controllo autorizzazione d'accesso ai sistemi gestionali	I sistemi gestionali disppngono di password di accesso che identifica l'operatore e ne associa un profilo di autorizzazione. La scadenza delle password avviene ogni 90 o 180 gioni in funzione della nautra sensibile o comune dei dati trattati. L'utente è in grado di definire autonomamente una nuova password. La lunghezza minima delle password, alfanumeriche, è di otto caratteri	Logica
02	Firewall	I dispositivi firewall sono presenti per proteggere la rete aziendale dall'esterno	Logica
03	Antivirus	I dispositivi dispongono di programmi antivirus.	Logica
04	Antispam	I servizi mail utilizati sono dotati di antispam	Logica
04	Autorizzazione accesso dominio	I client possono accedere al NAS solo attraverso una procedura di autenticazione informatica.	Logica
05	Password di accesso al client	L'accesso al client destinato al trattamento è protetto da nome utente e password	Logica

06	Screensaver	I client dispongono di salvaschermo che in caso di mancato utilizzo del computer oscurano il video e proteggono il terminale con password di sblocco	Logica
07	Controllo aggiornamento software	Con cadenza semestrale l'amministratore di sistema verifica gli aggiornamneti dei progammi utilizzati per il trattamento	Organizzativa
08	Isolamento da rete informatica	In alcuni casi si prevede di isolare il client dalla rete diminuendo il rischio di esposizione del computer ad attacchi dall'esterno o dall'interno della rete aziendale	Fisica
09	Backup su dispositivo magnetico e cloud	Il sistema di back-up esegue una copia giornaliera dei dati presenti su nas. È eseguita copia back-up dei dati in Cloud. È garantita la qualità delle copie di back-up e la loro conservazione in luogo adatto e sicuro	Logica
10	Collocazine copie back-up	Le copie sono custodite in stanza dedicata sotto la soveglianza del titolare del trattamento e/o dall'incaricato alla custodia delle aree, dei locali e degli archivi	Fisica
11	Collocazione e sorveglinza supporti cartacei	Gli schedari e altri supporti cartacei sono custoditi in stanza dedicata sotto la sorveglianza dall'incaricato alla custodia delle aree, dei locali e degli archivi. Nel caso in cui dovessero essere ricevuti terzi non autorizzati, i documenti cartacei eventualmente visibili sono riposti dallo stesso all'interno di archivi chiusi	Organizzativa
11	Istruzioni operative per gli incaricati al trattamento	Agli incaricati vengono date disposizioni, per iscritto per l'accesso ai soli dati, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbio è stato è stato loro prescritto di rivolgersi al titolare del trattamento. Gli incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative. Per quanto concerne l'archiviazione, sono state adibite apposite aree nelle quali conservare ordinatamente, documenti, atti e supporti, in modo distinto per le diverse funzioni aziendali.	Organizzativa
12	Controlli accessi	Nella sede aziendale è presente un incaricato alla custodia delle aree, dei locali e degli archivi preposta al controllo delle persone che accedono agli uffici. È presente un sistema di videosorveglianza esterno ai locali aziendali	Organizzativa e fisica
13	Chiusura locali	Le porte degli uffici sono chiuse nei momenti di pausa.	Fisica
14	Corsi di formazione	Sono previsti corsi per il personale coinvolto nel proceso di trattamento	Organizzativa
16	Divieti	All'interno dei locali è vietato fumare	Organizzativa

17	Controllo impianti	Gli impianti elettrici sono a norma	Fisica
13	Conservazione	I dati contenuti in supporti cartcei o informatici, scaduto il termine di conservazione, vengono distrutti. I dispositivi elettronici non più utilizzati sono smaltiti previa cancellazione dei dati personali ivi contenuti	Organizzativa
14	Aggiornamento	Le misure di sicurezza sono periodicamente verificate e aggiornate mediante l'utilizzo degli strumenti più idonei per la tutela dei dati trattati	Organizzativa
15	Controllo	Gli interessativi vengono prontamente avvisati qulora si verifichino situazioni anomale o emergenze	Organizzativa

8.4 ANALISI DEL RISCHIO

Tendo conto della probabilità e l'entità del danno, la presente tabella indica la valutazione dei rischi prima e dopo le misure di sicurezza adottate dall'azienda.

Fattori di rischio	Rischio (P x D = R)			Misure adottate	Rischio (P x D = R) Post Misura			Miglioramenti e priorità (vedi *infra* Cap. 8.5)
	P	D	**R**		P	D	**R**	
01	1	3	**3**	1/4/5/6/8/11	1	1	**1**	
02	2	3	**6**	1/2/3/4/7/8	2	1	**2**	
03	1	2	**2**	1/5/6/11	1	2	**2**	
04	2	4	**8**	1/2/3/5/6/7/9/11/12	1	2	**1**	
05	2	4	**8**	9/11/14	1	2	**1**	
06	1	2	**2**	3/7/9	1	1	**1**	
07	2	4	**8**	3/7/8	1	2	**2**	
08	1	2	**2**	1/2/4/6/12	1	2	**2**	
09	2	2	**4**	9/14	1	2	**2**	
10	2	2	**4**	11	1	2	**2**	
11	2	2	**4**	11	1	2	**2**	
12	1	4	**4**	16	1	2	**2**	
13	1	3	**3**	1/11/12/13	1	2	**2**	
14	1	3	**3**	11/14	1	2	**2**	
15	1	3	**3**	10/11/12/13	1	2	**2**	
16	2	2	**4**	9/14	1	2	**2**	
17	1	3	**3**	7/11	1	2	**2**	

8.5 CONTROLLO GENERALE SULLO STATO DI SICUREZZA E MIGLIORMANTO

Al titolare del trattamento è affidato il compito di aggiornare le misure organizzative e tecniche di sicurezza al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

Al fine di verificare l'efficacia delle misure di sicurezza, il titolare del trattamento, affidando l'incarico ad Auditor esterni preventivante qualificati, provvede, con frequenza annuale ad effettuare una o più delle seguenti attività:

(i) Verificare l'accesso fisico ai locali dove si svolge il trattamento

(ii) Verificare l'aggiornamento tecnologico delle risorse disponibili per il trattamento dei dati

(iii) Verificare la correttezza delle procedure di archiviazione e custodia di dati, documenti e supporto contenti dati
(iv) Verificare il livello di formazione delle persone incaricate al trattamento

I medesimi controlli potranno essere richiesti ed effettuati anche nei confronti di eventuali partner esterni, ovvero nei confronti dei Responsabili in outsourcing.

9. REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DEI DATI

Le dimensionie dell'azienda (<250 dipendenti) non impongono la tenuta del registro relativo ai trattmenti del Titolare come richiesto dall'art. 30.1 Reg. Ue 679/2016. Tuttavia, il titolare del trattamento, vista la non occasionalità del trattamento, visti i rischi per le libertà degli interessati, preso atto del parere Working Party 29, position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) del GDPR 19.4.2018, ha comunque predisposto un registro dei trattamenti costantemente aggiornato ed allegato al presente docomento.

10. ALLEGATI

- Lettera di incarico del responsabile per la protezione dei dati personali (*DPO*)
- Lettera di incarico amministratore di informativo aziendale
- Lettere di nomina responsabili esterni al trattamento dei dati personali
- Lettere di nomina incaricati interni al trattamento dei dati personali
- Lettera incarico alla custodia delle aree, dei locali e degli archivi cartacei
- Informazioni fornite agli interessati ai sensi dell'art. 13 Regolamento Ue 679/2016
- Registro dei trattamenti del titolare del trattamento

****

DICHIARAZIONE DI IMPEGNO E FIRMA

Il presente documento è firmato in calce dal sig. Gionata Graziotti (c.f. GRZGNT72M03C745Y), quale legale rappresentante pro tempore di White Label S.r.l., p.iva 03401510544, con sede legale in via Merlino Pazzaglia n. 7 – 06012 Città di Castello (Pg), pec whitelabel@pec.it, peo: amministrazione@whitelabelcompany.it www.dellafrancesca.store, tel. 057573385.

Sansepolcro (Ar), il 26/05/2020

White Label S.r.l.
Il legale rappresentante
Sig. Gionata Graziotti
……