DOCUMENTO PROGRAMMATICO PER LA SICUREZZA DEI DATI D.LGS. 196/03 e s.m.i.

DISPOSIZIONI MINIME SULLA SICUREZZA

Roma, 09 Ottobre 2018

Il Titolare del trattamento

_____

Rev.	Data	Motivo
0	11/12/2014	Prima emissione
1	15/02/2016	Aggiornamento per modello D.Lgs. 231/2001
2	14/07/2016	Aggiornamento cariche sociali
3	09/10/2018	Aggiornamento DPS

INDICE

Premessa

Il presente documento è redatto ai sensi del D.Lgs. n. 196/03 (Codice della privacy) del Disciplinare Tecnico allegato sub B, con lo scopo di descrivere il quadro delle misure minime di sicurezza, organizzative, fisiche e informatiche, adottate da **CFI – Cooperazione Finanza Impresa Scpa** (di seguito anche Titolare) con sede in Roma, Via G. Amendola 5, al fine della tutela dei dati personali trattati dall'azienda medesima presso la struttura stessa.
Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.
Il presente documento è approvato dal CdA.

1. Definizioni e responsabilità

AMMINISTRATORE DI SISTEMA E RESPONSABILE DELLA SICUREZZA INFORMATICA (di seguito ADS): il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione. In questo contesto l'ADS assume anche le funzioni di amministratore di rete, ovvero del soggetto che deve sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali.
È il soggetto preposto dal titolare alla gestione della sicurezza informatica. Il responsabile deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali.
Ai fini della sicurezza l'ADS, responsabile del sistema informativo, ha le responsabilità indicate dal provvedimento del Garante della Privacy del 27 novembre 2008 ("Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di ADS").

ACCESS LOG: si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un ADS o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi software.

CUSTODE DELLE PASSWORD: il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nella lettera di incarico.

DATI ANONIMI: i dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.

DATI PERSONALI: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

DATI IDENTIFICATIVI: i dati personali che permettono l'identificazione diretta dell'interessato.

DATI SENSIBILI: i dati personali idonei a rivelare 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, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

DATI GIUDIZIARI: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, 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.

INCARICATO: il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati. L'incaricato del trattamento dei dati, con specifico riferimento alla sicurezza, ha le responsabilità indicate nella lettera di incarico.

INTERESSATO: il soggetto al quale si riferiscono i dati personali.

RESPONSABILE DEL TRATTAMENTO: il soggetto preposto dal titolare al trattamento dei dati personali. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità indicate nella lettera di incarico.

TITOLARE: il titolare del trattamento è la CFI nella persona del suo Rappresentante legale, il Presidente del CdA, **Mauro Frangi**, tra i compiti che la legge gli assegna e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili e incaricati delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il titolare è il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

2. Titolare, responsabili, incaricati

Organigramma Privacy	***Nominativo***	
Titolare del trattamento	M. Frangi	
Responsabile del trattamento dei dati	C. De Berardinis A. Ruberti A. Viola F. Di Nuzzo C. Rocchi (Database) Modefinance (società esterna) Gaia Campus (legale esterno) Giuseppe De Angelis (consulente lavoro)	
Amministratore di Sistema e Responsabile sicurezza informatica	Dataworks S.a.s. di Dario Gasperoni	
Custode delle password	Dataworks S.a.s. di Dario Gasperoni	
Incaricati del trattamento dei dati	A. Danieli I. Esposito M. Lilli A. Castrichelli G. Cottarelli	M. Mariconda D. Stella C. Rocchi S. De Sanctis M. Staiano

3. Elenco dei trattamenti di dati personali

La CFI attua i seguenti trattamenti di dati personali:

01. trattamento di dati personali comuni[1] e sensibili[2] dei propri soci, connessi all'attività aziendale e comunque necessari, funzionali o connessi alla gestione del rapporto con le cooperative ed allo svolgimento dell'attività stessa, per le seguenti finalità:
☐ *organizzazione attività di istruttoria, attuazione e monitoraggio*
☐ *gestione erogazione partecipazione/finanziamenti - gestione dati economico-finanziari*
☐ *invio informative (posta, posta elettronica)*
☐ *gestione comunicazione tramite sito internet (www.cfi.it) ed email (info@cfi.it)*

02. trattamento di dati personali di fornitori, collaboratori, partner e professionisti (*commercialisti, avvocati, consulenti del lavoro, notai, etc.*), altre organizzazioni, enti pubblici, o comunque terzi con i quali la CFI ha periodico contatto, riguardanti la reperibilità e la corrispondenza con gli stessi, nonché richiesti ai fini fiscali o dati di natura bancaria o comunque necessari o funzionali allo svolgimento dell'attività dell'azienda;

03. trattamento di dati personali del personale dipendente, necessario alla gestione del rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesto ai fini fiscali o previdenziali o trattamento di dati di natura bancaria per le stesse finalità; trattamento di dati sensibili del personale dipendente, conseguenti al rapporto di lavoro[3], ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali, o all'adesione ad organizzazioni sindacali;

04. trattamento di eventuali dati giudiziari delle cooperative e dei dipendenti, idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, o idonei a rivelare la qualità di imputato o indagato, forniti dagli stessi o

[1] *Es. nominativo, residenza, numero telefonico, indirizzo e-mail, numero di cellulare, professione, studi compiuti……*
[2] *Es. eventuali indicazioni sui dati giudiziari dei soci*
[3] *Es. certificati di malattia, dati biometrici per gli accessi alla struttura*

da terzi, necessari o conseguenti allo svolgimento dell'attività, in accordo con quanto disposto dalla Autorizzazione del Garante n. 7/2012;

05. comunicazione[4] dei dati relativi alle cooperative finanziate/partecipate ai seguenti soggetti:
Ministero Sviluppo Economico, Centrali cooperative, per la finalità di: Pubblicazione dati relativi alle cooperative finanziate/partecipate.

06. diffusione[5] dei dati relativi alle cooperative finanziate/partecipate sul portale www.cfi.it per la finalità di ottemperare alle disposizioni del "Decreto Trasparenza".

I trattamenti possono comprendere il complesso di operazioni indicate nell'art. 4, comma 1, lett. a) Dlgs. 196/03 ed in particolare la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la cancellazione e la distruzione dei dati, nei limiti e con le modalità descritte nel presente documento e nell'informativa rilasciata all'interessato. La comunicazione dei dati avviene nei limiti di legge con riferimento a ciascun tipo di dato.

4. Strutture dove sono svolti i trattamenti, responsabili e distribuzione dei compiti

- I trattamenti ☒01 ☒02 ☒03 ☒04 ☒05 ☒06 vengono svolti presso la sede di Via G. Amendola [6].

Sono previsti i seguenti dispositivi di protezione degli accessi alla sede:
Portone di ingresso con chiusura blindata ☒
Sistemi di allarme antintrusione ☒
Dispositivi di lettura dati biometrici ☒ FINGER PASS, per accesso e registrazione entrata/uscita personale
Sono previsti i seguenti dispositivi di controllo dei locali in cui si trovano i ADS e gli archivi:
Porte con chiusura a chiave ☒
Armadi archivio con chiusura a chiave ☒
Sala server con chiusura a chiave e altri sistemi di protezione ☒ presso stanza dedicata

5. Modalità dei trattamenti

I trattamenti ☒01 ☒02 ☒03 ☒04 ☒05 ☒06 vengono svolti mediante i seguenti strumenti elettronici[7]:
☒ ADS e server connessi in rete ed a internet, contenenti[8] *:*

☒ banca dati dipendenti/collaboratori
☒ banca dati fornitori
☐ banca dati clienti (nome banca dati): Database Modefinance

Per una descrizione dettagliata si fa riferimento all'Allegato 1 – Sintesi del sistema informatico Dataworks
In allegato sono disponibili:

- piantine sedi e uffici con layout del sistema informatico
- inventario hardware in dotazione
- inventario software in dotazione
- inventario altre attrezzature per la sicurezza in dotazione
- I trattamenti ☒01 ☒02 ☐03 ☐04 ☒05 ☒06 sono svolti anche mediante archivi e strumenti cartacei.

[4] *D. lgs. 196/03 lett. l "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*
[5] *D. lgs. 196/03 lett.m "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*
6 Selezionare i trattamenti effettuati e le misure in essere
[7] *La descrizione qui sotto è solo esemplificativa. L'azienda può anche ovviamente avere un solo ADS non collegato alla rete, o non avere strumenti elettronici. Per le misure di sicurezza da adottare si veda anche la "nota tecnica".*
[8] *Indicare la banca dati esistente nel ADS (es. elenco clienti, elenco dipendenti ……).*

Codice banca dati	Descrizione	Categoria dati trattati e soggetti a cui si riferiscono	Luogo di custodia	Finalità del trattamento	Modalità trattamento	Descrizione strumenti utilizzati	Comunicazione (si/no)	Diffusione (si/no)	Procedura di Backup	Trasferibile su supporto rimovibile	Responsabile trattamento
Database Modefinance	Gestione stato e archiviazione dell'iter delle pratiche e relative fasi di istruttoria, attuazione e monitoraggio	Dati personali dei soci delle cooperative, dati comuni (anagrafica, dati bancari, ecc.)	Informatico e su server delocalizzato, gestito da ModeFinance	Gestione del credito e del rischio, archiviazione e monitoraggio pratiche	raccolta, ricezione e registrazione di dati o acquisizione, stampa documenti finalizzati alla attuazione delle pratiche	Cruscotto software su ogni Computer incaricato e il Database centralizzato	NO	NO	Backup del database ogni 24 ore copiando i dati su uno storage Amazon. I backup salvati sono uno ogni mese per gli ultimi 6 mesi, uno ogni settimana per le ultime 5 settimane, uno ogni giorno per gli ultimi 7 giorni	**NO**	**ModeFinance C. Rocchi**
Cartelle di lavoro	Cartelle che contengono file e documenti di lavoro, report archiviati su ADS in locale di ogni incaricato nello svolgimento delle attività	Dati personali dei soci delle cooperative, dati comuni (anagrafica, dati bancari, finanziari, sociali, ecc.)	informatico e su server, cartaceo in archivio chiuso e protetto	Predisposizione documenti per lavorazione pratica e successiva archiviazione su DB ModeFinance		Cartelle su ADS degli incaricati	**NO**	**NO**	Rif.Allegato 1 – Sintesi Dataworks	**NO**	**Lista Responsabili**
Archivio server istruttoria	Cartelle che contengono file relativi all'attività, archiviate su server	Dati personali dei soci delle cooperative, dati comuni (anagrafica, dati bancari, finanziari, sociali, ecc.)	informatico e su server			Cartelle dedicate su Permanent file (archivio server)	**SI**	**SI**		**NO**	**Lista Responsabili**
Archivio server attuazione	Cartelle che contengono file relativi all'attività, archiviate su server	Dati personali dei soci delle cooperative, dati comuni (anagrafica, dati bancari, finanziari, sociali, ecc.)	informatico e su server				**SI**	**SI**		**NO**	**Lista Responsabili**

Archivio server monitoraggio	Cartelle che contengono file relativi all'attività, archiviate su server	Dati personali dei soci delle cooperative, dati comuni (anagrafica, dati bancari, finanziari, sociali, ecc.)	informatico e su server				**SI**	**SI**		**NO**	**Lista Responsabili**
Permanent file	DB di archiviazione di tutte le Cartelle che contengono file relativi all'attività e alle pratiche per le cooperative, archiviate su server	Dati personali dei soci delle cooperative, dati comuni (anagrafica, dati bancari, finanziari, sociali, ecc.)	informatico e su server	Archiviazione documenti relativi la cooperativa	Raccolta, conservazione, archiviazione		**NO**	**NO**		**NO**	**Lista Responsabili**
Programma CORA	Accensione ed estinzione rapporti con società cooperative	Dati anagrafici e tipologia di operazione per singola coop.	informatico e su server	Gestione del rapporto per la comunicazione all'Agenzia delle Entrate	raccolta, ricezione e registraz.ne o acquisizione, stampa	**Software Star Infostudio**	**SI**	**NO**		**NO**	**Lista Responsabili**
DB contabilità	Database della contabilità	Dati contabili gestione amministrativa	informatico e su server	Gestione contabilità ordinaria	raccolta, ricezione e registrazione o acquisizione, stampa	**Software DB**	**SI**	**SI**		**NO**	**Lista Responsabili**
DB Cerved	Banche dati pubbliche	Dati centrali di rischio	informatico e su server	Consultazione informazioni relative alle cooperative	Interrogazione, visualizzazione, stampa	**Internet**	**SI**	**SI**		**NO**	**Lista Responsabili**

6. Analisi dei rischi incombenti sui dati

Analisi dei rischi – approccio metodologico

Come è noto, il Documento Programmatico sulla Sicurezza (DPS) deve contenere (regola 19 dell'allegato B, "Disciplinare tecnico in materia di misure minime di sicurezza", del D. Lgs. n.196) "l'analisi dei rischi che incombono sui dati personali e le tutele da adottare per prevenire la loro distruzione, l'accesso abusivo e la dispersione".
Il Garante stesso, inoltre, ha pubblicato, nel marzo 2004, la "Guida operativa per redigere il Documento programmatico sulla sicurezza" che propone il seguente approccio metodologico, adottato dalla CFI per la gestione della privacy:

1. individuazione dei principali eventi potenzialmente pregiudizievoli per il trattamento dei dati personali;
2. valutazione dei possibili impatti di tali eventi;
3. elencazione delle contromisure di sicurezza adottate a fronte dell'analisi eventi / impatti.

Eventi pregiudizievoli

Il Garante propone la seguente lista di eventi potenzialmente dannosi:

1. Contesto fisico-ambientale

- Ingressi non autorizzati a locali/aree ad accesso ristretto
- sottrazione di strumenti contenenti dati
- eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria
- guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)
- errori umani nella gestione della sicurezza fisica

Rischi relativi alla Infrastruttura	Rischi relativi alle comunicazioni
Mancanza di protezione fisica dell'edificio (porte finestre ecc.) Mancanza di controllo di accesso Linea elettrica instabile Locazione suscettibile ad allagamenti	Linee di comunicazione non protette Giunzioni non protette Mancanza di autenticazione Trasmissione password in chiaro Mancanza di prova di ricezione/invio Presenza di linee dial-up (con modem) Traffico sensibile non protetto Gestione inadeguata della rete Connessioni a linea pubblica non protette

2. Comportamenti degli operatori

- Sottrazione di credenziali di autenticazione;
- carenza di consapevolezza;
- disattenzione o incuria;
- comportamenti sleali o fraudolenti;
- errore materiale.

Rischi relativi al personale
Mancanza di personale Mancanza di supervisione degli esterni Formazione insufficiente sulla sicurezza Mancanza di consapevolezza Uso scorretto di hardware/software Carenza di monitoraggio Mancanza di politiche per i mezzi di comunicazione Procedure di reclutamento inadeguate Carenza di controllo di configurazione Mancanza di copie di backup

3. Eventi relativi agli strumenti

- Azione di virus informatici o di programmi suscettibili di recare danno;
- spamming o tecniche di sabotaggio;
- malfunzionamento, indisponibilità o degrado degli strumenti;
- accessi esterni non autorizzati;

- intercettazione di informazioni in rete.

Rischi relativi all'Hardware
Mancanza di sistemi di rimpiazzo
Suscettibilità a variazioni di tensione
Suscettibilità a variazioni di temperatura
Suscettibilità a umidità, polvere, sporcizia
Suscettibilità a radiazioni elettromagnetiche
Manutenzione insufficiente
Carenze di controllo di configurazione (update/upgrade dei sistemi)
Rischi relativi ai Software
Interfaccia uomo-macchina complicata
Mancanza di identificazione /Autenticazione
Mancanza del registro delle attività (log)
Errori noti del software
Tabelle di password non protette
Carenza/Assenza di password management
Scorretta allocazione dei diritti di accesso
Carenza di controllo nel caricamento e uso di software
Permanenza di sessioni aperte senza utente
Carenza di documentazione
Incuria nella dismissione di supporti riscrivibili

Valutazione del rischio

Per valutare il rischio degli eventi potenzialmente pregiudizievoli, considerati i danni per l'azienda in caso di perdita di Riservatezza, Integrità e Disponibilità delle informazioni gestite, è usata una scala di "gravità" molto semplice:

- Livello 4: rischio gravissimo (vitale per l'azienda);
- Livello 3: rischio molto grave;
- Livello 2: rischio importante;
- Livello 1: rischio non significativo.

Con riferimento alla struttura, i rischi possono consistere in ingressi di estranei a locali/aree, nella sottrazione di strumenti contenenti dati, in eventi distruttivi naturali (es. incendi, allagamenti, condizioni ambientali, ...), o artificiali (es. guasto di sistemi complementari), in errori umani nella gestione della sicurezza fisica.
Tali rischi possono esser definiti in massima parte di livello 2, poiché presso la sede ci sono misure di sicurezza efficienti, come indicato nella *tabella n.2*, in particolare: è sempre garantita la presenza di personale, l'accesso di estranei è controllato costantemente **anche mediante un sistema di videosorveglianza delle porte di ingresso**, l'impianto elettrico è dotato di dispositivo salvavita. Inoltre, sono stati posti in sede diversi estintori i quali sono regolarmente manutenuti.
Con riferimento agli strumenti elettronici, i rischi possono essere definiti in massima parte di livello 2, essendo state adottate le misure di sicurezza minime specificate nella *tabella n.2*, che sono altresì costantemente aggiornate.

Tabella 1. Valutazione dei rischi

Ambito	Evento	Rischio
1. Contesto fisico-ambientale	Ingressi non autorizzati a locali/aree ad accesso ristretto	2
	sottrazione di strumenti contenenti dati	2
	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria	1
	guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)	2

	errori umani nella gestione della sicurezza fisica	2
2. Comportamenti degli operatori	Sottrazione di credenziali di autenticazione;	1
	carenza di consapevolezza;	3
	disattenzione o incuria;	3
	comportamenti sleali o fraudolenti;	2
	errore materiale.	2
3. Eventi relativi agli strumenti	Azione di virus informatici o di programmi suscettibili di recare danno;	4
	spamming o tecniche di sabotaggio;	4
	malfunzionamento, indisponibilità o degrado degli strumenti;	3
	accessi esterni non autorizzati;	3
	intercettazione di informazioni in rete.	2

7. Misure di sicurezza per il trattamento con strumenti elettronici adottate

Tabella 2. Misure di sicurezza adottate

Ambito	Evento	Rischio	Contromisura
1. Contesto fisico-ambientale	Ingressi non autorizzati a locali/aree ad accesso ristretto	2	Sorveglianza alla reception, badge per l'ingresso al piano, lettori biometrici, **sistema di videosorveglianza con registrazione**
	sottrazione di strumenti contenenti dati	2	Sorveglianza alla reception, badge per l'ingresso al piano, lettori biometrici
	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria	1	Schedulazione di backup (rif. Allegato 1 Sintesi Dataworks)
	guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)	2	Dotazione di gruppi di continuità (ups)
	errori umani nella gestione della sicurezza fisica	**1**	Formazione – Istruzione agli incaricati
2. Comportamenti degli operatori	Sottrazione di credenziali di autenticazione;	1	Cambio credenziali semestrale password (rif. Allegato 1 Sintesi Dataworks)
	carenza di consapevolezza;	3	Formazione – Istruzione agli incaricati
	disattenzione o incuria;	3	Formazione – Istruzione agli incaricati
	comportamenti sleali o fraudolenti;	1	Controlli automatici e manuali (rif. Allegato 1 Sintesi Dataworks)
	errore materiale.	2	Formazione – Istruzione agli incaricati, controlli automatici e manuali
3. Eventi relativi agli strumenti	Azione di virus informatici o di programmi suscettibili di recare danno;	4	Sistema antivirus centralizzato **+ recupero dati da backup** (rif. Allegato 1 Sintesi Dataworks)
	spamming o tecniche di sabotaggio;	4	Filtri antispam sulla posta in entrata (rif. Allegato 1 Sintesi Dataworks)
	malfunzionamento, indisponibilità o degrado	3	Schedulazione di backup (rif.

	degli strumenti;		Allegato 1 Sintesi Dataworks)
	accessi esterni non autorizzati;	3	Firewall (rif. Allegato 1 Sintesi Dataworks)
	intercettazione di informazioni in rete.	2	Firewall (rif. Allegato 1 Sintesi Dataworks)

7.1 Istruzioni per gli incaricati

Gli incaricati dei trattamenti di dati personali devono scrupolosamente attenersi alle seguenti istruzioni.

a) Principi generali
I dati personali devono essere sempre trattati in modo lecito e secondo correttezza. Essi devono essere raccolti, classificati e registrati per scopi determinati, funzionali all'attività dell'azienda, espliciti e legittimi.
Tutto il personale è tenuto ad attivarsi per far sì che i dati trattati siano esatti e per quanto possibile aggiornati. I trattamenti non devono mai eccedere le finalità per le quali sono stati concepiti.
I dati devono essere conservati limitatamente al periodo necessario in relazione agli scopi per i quali sono raccolti (salvo quanto previsto da altre disposizioni di legge). Trascorso tale periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita

b) Riservatezza dei dati personali
Gli incaricati devono sempre usare, all'interno come all'esterno della CFI, la massima discrezione sui dati personali di cui siano a conoscenza, curando attentamente la loro protezione.
Anche le comunicazioni tra colleghi di dati personali di terzi devono limitarsi a quanto necessario per l'espletamento delle proprie mansioni.
È vietata ogni comunicazione di dati all'esterno dell'azienda, salvo il caso in cui ciò sia necessario per lo svolgimento degli incarichi affidati.
La fase di raccolta del consenso dovrà essere preceduta dalla informativa ed il consenso degli interessati, raccolto preferibilmente in forma scritta. È obbligatorio il consenso scritto se riguarda i dati sensibili.
Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.
Se il trattamento di dati è effettuato in violazione di quanto disposto dal codice della privacy è necessario provvedere al "blocco" dei dati (sospensione temporanea di ogni operazione di trattamento) fino alla regolarizzazione del trattamento (ad es. fornendo l'informativa omessa o raccogliendo il consenso non dato) ovvero alla cancellazione dei dati se non è possibile regolarizzare.

c) Utilizzo del materiale (Computer e programmi)
Gli incaricati sono tenuti ad utilizzare esclusivamente strumenti e programmi forniti o autorizzati dalla CFI e soltanto per svolgere le proprie mansioni. È vietato l'utilizzo di altri supporti o di programmi non autorizzati. I dispositivi (terminali e COMPUTER) devono essere disattivati durante le assenze (comprese le pause) dell'utente.
Le misure adottate da CFI per la protezione/prevenzione dai rischi connessi al trattamento elettronico dei dati sono descritte nella sezione 7 del presente documento e nell'Allegato 1 – Sintesi Dataworks.

d) Utilizzo di password e username
Ad ogni dipendente è assegnata una username (identificativo utente) e password (parola chiave) personali, necessarie per accedere agli elaboratori e ai dati in essi contenuti. Il medesimo username non può, nemmeno in tempi diversi, essere assegnato a persone diverse.
La password deve essere mantenuta segreta verso chiunque, compresi i colleghi di lavoro. A tale scopo è vietata l'evidenziazione o la memorizzazione della password con biglietti, messaggi e ogni altra modalità che ne comprometta la segretezza.
Ove si rendesse necessaria l'assegnazione di nuove credenziali di accesso è fatto obbligo al personale di rivolgersi unicamente all'ADS.
L'utilizzo combinato di username e password attribuisce in modo univoco al loro titolare la responsabilità delle operazioni compiute.

La password può essere sostituita in ogni momento nel rispetto di quanto sopra. Deve essere sostituita ogni **6 mesi** qualora non diversamente specificato nella lettera di incarico o nelle procedure aziendali, nonché quando vi sia anche il semplice sospetto che ne sia venuta meno la segretezza verso chiunque.
La gestione delle password è riservata all'ADS Responsabile della Sicurezza. In caso di dimenticanza, di anomalie o quando se ne dovesse ritenere l'opportunità, è sempre possibile richiederne il reset. L'ADS assegna una password che rispetti i requisiti minimi di complessità (lunghezza minima 8 caratteri alfanumerici che non contenga parole di vocabolario o qualsiasi dato riconducibile all'incaricato) tramite l'ausilio di apposito software. A garanzia ulteriore della privacy dei dati, il sistema è impostato in modo che, nel caso in cui l'utente lasci il proprio Computer inattivo per alcuni minuti, si determina il blocco della postazione e la richiesta di inserimento password per la riattivazione delle funzionalità.

e) Archivio e gestione dei documenti
Tutti i documenti cartacei devono essere gestiti in modo da ridurre al minimo i tempi di permanenza al di fuori degli archivi, armadi o contenitori posti nei locali della CFI.
Massima attenzione dovrà essere posta per i documenti che si trovano in locali accessibili al pubblico. Nei giorni di accesso del personale agli uffici la documentazione dovrà essere riposta negli appositi contenitori (armadi ignifughi, cassettiere e schedari chiusi a chiave) e non dovranno essere lasciati incustoditi gli uffici al cui interno vi sia personale non autorizzato.
L'accesso agli archivi è consentito al personale incaricato, a ciò espressamente autorizzato in via permanente od occasionale.
Gli archivi devono essere mantenuti costantemente chiusi, compatibilmente con le esigenze di servizio.
Le copie dei documenti vanno trattate, con riferimento alla tutela dei dati personali in esse contenuti, con la medesima diligenza riservata agli originali.
Gli addetti ai servizi dove possono essere trattati dati sensibili o giudiziari dovranno porre massima attenzione al rispetto delle disposizioni precedenti.
Gli incaricati, inoltre, dovranno limitare al minimo indispensabile la giacenza della documentazione al di fuori degli armadi o contenitori muniti di serratura e controllare con particolare rigore l'accesso ai propri archivi. Solamente il Responsabile del trattamento potrà autorizzare l'accesso agli archivi al di fuori dell'orario di lavoro e ciò dovrà essere dallo stesso registrato in apposito documento.
I supporti cartacei, contenenti dati personali e/o sensibili, a fine ciclo lavorativo devono essere archiviati in locale ad accesso controllato.

f) Accesso ai Computer
L'accesso ai terminali ed ai PC portatili è consentito solo ai dipendenti della CFI; l'eventuale accesso di terzi è consentito solo se precedentemente autorizzati dal titolare del trattamento e dall'ADS, comunque mai utilizzando le credenziali dell'utilizzatore abituale del COMPUTER (vedi sistema per accessi alla rete di esterni). Per consentire l'accesso di terzi senza creare pericoli per il sistema informativo sono state adottate alcune misure descritte *nell'Allegato 1 – Sintesi Dataworks*.
L'ADS Responsabile della sicurezza è autorizzato a procedere in qualunque momento, alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza dei COMPUTER degli incaricati sia sulle unità di rete.
È opportuno che con regolare periodicità ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili o duplicati, al fine di evitare il rischio di un'archiviazione ridondante.
L'accesso ai computer è consentito in remoto solo all'ADS (su autorizzazione dell'utente) ed esclusivamente per le operazioni di supporto tecnico.

Uso di PC portatili
L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo sul luogo di lavoro. I PC portatili possono accedere tramite autenticazione (per mezzo di un voucher temporaneo) alla rete Wireless di CFI, tale accesso è limitato esclusivamente alla navigazione in internet e non all'accesso alle risorse della rete locale (es. servers, stampanti, etc). Nel caso il PC portatile venga autorizzato all'accesso alle risorse della rete locale verrà trattato come previsto per i Computer fissi.

Di seguito un riepilogo delle misure di sicurezza in uso.
- ciascun incaricato viene dotato dall'ADS di un proprio username e di una password. La password rispetta i requisiti minimi di complessità e non contiene elementi facilmente ricollegabili all'incaricato. La nuova password viene memorizzata dall'incaricato e custodita in un luogo che garantisca la segretezza. Ogni sei mesi le password saranno modificate dall'ADS e comunicate esclusivamente agli interessati.

- È disposto che tutti gli incaricati non lascino incustodito o accessibile il PC. A tale riguardo, per evitare errori e dimenticanze, il sistema è impostato in modo che, nel caso in cui l'utente lasci il proprio PC inattivo per alcuni minuti, si determina il blocco della postazione e la richiesta di inserimento password per la riattivazione delle funzionalità[9].
- Per eliminare e/o limitare il rischio di intrusione e azione di programmi (virus, trojan horse, malware, spyware, ecc.), tutti i PC sono dotati di antivirus con funzione di aggiornamento automatico e sistema centralizzato di monitoraggio. È fatto obbligo per tutti gli utenti di tenere comportamenti tali da ridurre il rischio di attacco informatico mediante virus o altro software aggressivo. Ogni dispositivo di provenienza esterna deve essere verificato mediante il programma antivirus installato prima di essere utilizzato e nel caso venga rilevato un virus deve essere consegnato all'ADS.
- Per ogni singolo PC sarà compiuta, con scadenza programmata, la funzione di aggiornamento del sistema operativo mediante lo strumento di update automatico;
- Con riferimento ai supporti rimovibili, se contenenti dati sensibili o giudiziari, è stato disposto che siano custoditi in cassetti chiusi a chiave e, se non più utilizzati, siano distrutti o resi inutilizzabili. È vietato l'uso di supporti rimovibili personali;
- Sarà inoltre adottata ogni altra misura che venisse ritenuta utile e necessaria dai tecnici, compatibilmente alle risorse dell'Azienda, per migliorare la sicurezza degli strumenti elettronici.

g) Utilizzo e manutenzione della posta elettronica

Gli indirizzi aziendali possono essere utilizzati solamente per finalità strettamente lavorative.
Per l'utilizzo privato della posta tutti i lavoratori sono invitati ad avvalersi di servizi di webmail.
È fatto divieto di utilizzare le caselle di posta elettronica ufficiali per:

- Invio/ricevimento di allegati contenenti filmati o brani musicali non legati all'attività lavorativa
- Invio/ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, scommesse, forum o mailing-list
- Partecipazione a catene telematiche (tipo Sant'Antonio). Non si dovrà in nessun caso procedere all'apertura di tali allegati

La casella di posta deve essere mantenuta in ordine e priva di allegati inutili, specie se ingombranti.
È obbligatorio porre la massima attenzione nell'aprire allegati o link contenuti in messaggi di posta elettronica, e di non scaricare programmi e/o file eseguibili da internet senza il preventivo consenso dell'ADS.

La posta elettronica può essere controllata dal datore di lavoro (attraverso l'ADS) senza preventiva comunicazione, ogni volta si ravvisi, un pericolo per l'integrità del sistema informatico (es. un attacco di virus informatici) o se questo è necessario per la legittima tutela della CFI e comunque nel rispetto di quanto stabilito nella **Provvedimento del Garante per la Privacy in data 01/03/2007 n. 13**, G.U. 10.03.2007.
Durante i periodi di assenza programmata dal lavoro il lavoratore dovrà inserire nel testo della mail un messaggio di risposta automatico contenente le coordinate di un indirizzo alternativo.
La posta elettronica collegata agli uffici è automaticamente conservata in apposite cartelle di posta del server.
Nel caso di cessazione del rapporto di lavoro dell'utente, i dati della casella di posta vengono salvati dall'ADS ed archiviati e conservati per un tempo stabilito.

g) Utilizzo di internet

Internet può essere utilizzato tenendo conto delle limitazioni riepilogate di seguito.
CFI, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, quali l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee all'attività), adotta opportune misure che possono, così, prevenire controlli successivi sul lavoratore:

- configurazione di sistemi o utilizzo di filtri che impediscono determinate operazioni –reputate incoerenti con l'attività lavorativa – quali l'upload e il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

È fatto espresso divieto di:

[9] *Lo screensaver con password è consigliato ma non obbligatorio.*

- scaricare software gratuiti (freeware e shareware)
- effettuare ogni genere di transazione finanziaria, comprese le azioni di remote banking o acquisti on-line e simili, fatti salvi i casi autorizzati in relazione alle mansioni svolte
- ogni forma di registrazione a siti internet cui contenuti non siano strettamente legati all'attività lavorativa
- la partecipazione a forum non professionali, chat e simili anche usando pseudonimi (o nicknames) espressamente autorizzati dal Responsabile del trattamento.

Gli eventuali controlli, compiuti dall'ADS o personale tecnico incaricato, potranno avvenire attraverso un sistema di controllo dei contenuti (proxy server) o mediante file log.

h) Utilizzo di fax, stampanti , scanner e fotocopiatrici, smartphone

è vietato l'utilizzo dei fax per ricevere e spedire documenti personali, nonché l'uso di stampanti e fotocopiatrici per usi estranei all'attività lavorativa. È fatto divieto, inoltre, di scansionare documenti personali**.**

È fatto esplicito divieto a tutti di copiare o trasferire dati aziendali di qualsiasi natura con o senza l'ausilio di strumenti informatici quali hd esterni, pen drive usb, bluetooth, dvd, cd, smartphone, tablet, ecc., né in allegato via posta elettronica o attraverso servizi ftp, sistemi peer-to-peer, senza essere espressamente autorizzati dall'ADS.

Per i dispositivi mobili aziendali (telefoni cellulari, tablet, smartphone) in dotazione o personali, aventi accesso a reti, dati e sistemi aziendali, è fatto divieto di:

- utilizzare il sistemi operativi diversi da quelli autorizzati dall'ADS;
- modificare/eliminare le password salvate dall'utente;
- caricare sul o sui dispositivi dati non essenziali allo svolgimento del proprio lavoro;
- sottoporre i dispositivi ad installazioni di software/firmware allo scopo di accedere a funzionalità il cui uso non è destinato all'utente;
- scaricare sui dispositivi copie pirata di software, o contenuti illegali;
- installare applicazioni da non fonti ufficiali o non approvate dai vendor della piattaforma. È severamente vietato installare codice proveniente da fonti non attendibili. In caso di dubbio sull'attendibilità dell'origine di un'applicazione, l'ADS di CFI;
- connettere un dispositivo a un ADS privo di protezione antivirus aggiornata e abilitata, e non conforme ai criteri aziendali;
- inviare i dati aziendali al di fuori del sistema di posta elettronica aziendale. Se un utente sospetta che siano stati inviati dati aziendali da un account e-mail personale, nel corpo del messaggio o come allegato, ha il dovere di informare immediatamente l'ADS.
- Agli utenti non è consentito utilizzare le postazioni di lavoro aziendali per il backup o la sincronizzazione di contenuti del dispositivo come file multimediali, a meno che tali contenuti siano necessari per il legittimo svolgimento delle proprie mansioni lavorative.
- Ad eccezione dei dispositivi gestiti dall'ADS, non è consentita la connessione diretta dei dispositivi alla rete aziendale interna.

i) Accesso ai dati trattati dall'utente

È facoltà del Titolare del trattamento, per motivi di sicurezza che tecnici e/o manutentivi, comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, tramite l'ADS, accedere direttamente, nel rispetto della normativa vigente in materia di privacy, a tutti gli strumenti informatici e ai documenti ivi contenuti presenti presso CFI.

In caso di anomalie, l'ADS, effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia. Controlli su base individuale saranno effettuati solo successivamente a ulteriori anomalie. In nessun caso saranno compiuti controlli prolungati, costanti o indiscriminati.

l) Sanzioni

L'inosservanza delle norme poste a tutela dei dati personali può determinare l'insorgere di responsabilità di tipo disciplinare, civile o anche penale, con l'applicazione – ove ne ricorrano i presupposti – delle relative sanzioni, oltre all'eventuale risarcimento del danno cagionato.

8. Misure di sicurezza per i trattamenti non elettronici

Rischi per dati su supporto cartaceo
Locali documenti non protetti Carenza di precauzioni nell'eliminazione Non controllo delle copie

Per ridurre i rischi relativi al trattamento cartaceo e manuale sono state adottate le seguenti misure:

- Si è disposto che gli incaricati non lascino incustoditi sulle scrivanie, o su altri ripiani o in luoghi accessibili all'utenza o al pubblico atti, documenti e fascicoli contenenti dati personali, ma li conservino in appositi schedari/fascicoli, prelevandoli solo per il tempo necessario al trattamento e poi restituendoli.
- Il locale destinato all'archivio sarà chiuso a chiave. Il custode è il Responsabile ed è incaricato di controllare l'accesso all'archivio. Fuori dall'orario di apertura della sede l'accesso all'archivio sarà consentito previa autorizzazione espressa, qualora l'archivio contenga dati sensibili o giudiziari.

8.1 Misure per il Disaster Recovery e ripristino dei dati

Nell'ipotesi di distruzione o danneggiamento dei dati sensibili o degli strumenti elettronici che li contengono si adotterà la seguente procedura:

- gli incaricati avvertiranno il titolare*/responsabile* o direttamente l'ADS, che ha accesso esclusivo alle copie di backup ed ai supporti elettronici contenenti i software installati nei ADS distrutti o danneggiati;
- il titolare/responsabile chiederà immediatamente l'intervento dell'ADS sollecitandone al più presto l'assistenza;
- l'ADS provvederà a reinstallare i programmi danneggiati o distrutti, o a sostituire il disco fisso o l'intero hardware, reinstallandovi il sistema operativo e i dati e programmi contenuti nelle copie di backup e provvedendo al loro aggiornamento;

In ogni caso, viene data esplicita istruzione che il ripristino dei dati venga effettuato entro e non oltre 7 giorni dalla distruzione o danneggiamento.

8.2 Backup

I dati sono soggetti a precise procedure di backup, dettagliate **nell'Allegato 1 – Sintesi DATAWORKS**
Tutte le banche dati elettroniche sono soggette giornalmente a backup automatici dei dati.
Le copie vengono eseguite su unità dedicata collocata sul server centrale.

9. Formazione degli incaricati

La formazione degli incaricati verrà effettuata all'atto della nomina e dell'assunzione dei compiti relativi, in caso di installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale. Ogni incaricato riceve inoltre una lettera di incarico contenente i suoi compiti, le istruzioni operative e i limiti del suo trattamento. Potranno essere indetti specifici corsi, destinati a coloro i quali svolgono il trattamento di dati sensibili. La formazione tende a sensibilizzare gli incaricati sulle tematiche della sicurezza, facendo comprendere i rischi e le responsabilità in cui incorrono (con specificazione delle sanzioni amministrative, penali e disciplinari). Inoltre, essa consiste nella spiegazione del concetto di "dato sensibile", nell'invito a segnalare eventuali disfunzioni dei sistemi operativi e, nel dubbio, di richiedere al titolare e al Responsabile ogni chiarificazione o istruzione. La formazione è svolta dal Responsabile. [10]

10. Trattamento da parte di soggetti esterni

Il trattamento relativo alla gestione delle paghe e contributi dei dipendenti, contabili e fiscali è svolto all'esterno, avvalendosi della collaborazione dello studio Associato De Angelis.
Il trattamento relativo alla gestione degli affari legali è svolto all'esterno, avvalendosi della collaborazione dello studio Avv. Gaia Campus.

Tali soggetti sono nominati Responsabili di quello specifico trattamento[11]. Tali soggetti offrono piena garanzia per il corretto assolvimento del proprio compito, assumono l'obbligo di utilizzare i dati solo per lo scopo a loro assegnato, dichiarano di adottare le misure di sicurezza previste dal Codice e di relazionare periodicamente all'Azienda sulle misure di sicurezza adottate.

---

[10] *La formazione degli incaricati è obbligatoria per legge. Se si tratta di dipendenti o personale stabile a costoro va formalizzata. In ogni caso, è essenziale che gli incaricati sappiano utilizzare la loro password e sappiano quali trattamenti possono svolgere e quali sono vietati. Nel fare la formazione ci si può basare sul contenuto del DPS ed eventualmente integrarlo. Si ricorda che, in ogni caso, i compiti (e quindi anche i limiti) per un incaricato devono emergere nella lettera di incarico a lui consegnata.*

[11] *La nomina del soggetto esterno quale Responsabile è facoltativa.*

11. Nomina ed elenco degli Amministratori di Sistema

CFI ha nominato quale Amministratore di sistema e Responsabile della sicurezza dei dati la DATAWORKS S.a.s. di Dario Gasperoni, che svolge le funzioni ad essa attribuite con formale incarico, mediante le seguenti persone fisiche/tecnici:
1. Dario Gasperoni

12. Lista dei Responsabili e degli incaricati al trattamento dei dati personali

Codice Archivio	Responsabile del trattamento	Incaricato
DBModefinance	C. Rocchi/Modefinance	Tutti gli incaricati
Cartelle di lavoro	Tutti i Responsabili	Tutti gli incaricati
Archivio server istruttoria	A. Viola	I. Esposito, M. Mariconda
Archivio server attuazione	F. Di Nuzzo	S. De Sanctis
Archivio server controllo/monitor.	F. Di Nuzzo	A. Danieli, A. Castrichelli
Archivio server amministrazione	A. Ruberti	C. Rocchi, D. Stella
Permanent file	Tutti i Responsabili	Tutti gli incaricati
Programma CORA	Rappresentante legale	C. Rocchi
DB contabilità	A. Ruberti	C.Rocchi, D.Stella
DB Cerved	Tutti i Responsabili	Tutti gli incaricati

13. Aggiornamento

Il documento in oggetto non deve rimanere statico ma deve essere aggiornato ogni volta che vi siano cambiamenti significativi nella società impattanti sulle misure minime di sicurezza.
Il presente DPS è conservato presso la sede della CFI, per essere esibito in caso di controllo, è a disposizione di ogni incaricato e verrà aggiornato **ogni qual volta lo si ritenesse necessario**.

14. Allegati

- Allegato 1 – Sintesi Dataworks
- Nomina Amministratore di Sistema e Responsabile della Sicurezza Informatica

ROMA, 09/10/2018

Il legale rappresentante

I Responsabili del trattamento