REGOLAMENTO DI ANALISI

SULLA SICUREZZA E TRATTAMENTO DEI DATI

(GDPR 2016/679/UE)

MODELLO ORGANIZZATIVO PRIVACY

Ser.In.Ar. S.C.P.A.	**Registro delle attività di trattamento dati** ai sensi dell'art. 30 del Reg. CE 27-4-2016 2016/679/UE	
Indirizzo: **Via Corridoni,18** **47121 Forlì**	Data: **10/01/2019**	
Revisione N° 2.0	Tel.: **0543 375511**	Partita IVA: **01940960402** e-mail: serinar@criad.unibo.it pec: serinar@legalmail.it

INDICE

1 PREMESSA

Il presente documento, adottato da Ser.In.Ar.(d'ora in avanti anche più semplicemente Società) conformemente al GDPR 2016/679/UE (REGOLAMENTO DEL PARLAMENTO EUROPEO relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati), in materia di protezione dei dati personali (anche con riferimento alle categorie dei dati particolari e dei dati giudiziari) trattati con l'ausilio di strumenti elettronici o manuali, ha lo scopo di fornire un quadro, il più possibile strutturato, del sistema privacy adottato e delle conseguenti azioni volte a garantire la *compliance* alla normativa privacy. Tali azioni mirano a contenere, entro limiti accettabili, il rischio di: distruzione, anche accidentale (perdita della disponibilità), accesso non autorizzato (compromissioni dell'integrità e della riservatezza), trattamento non consentito o non conforme alle finalità della raccolta, dei dati personali in possesso della Società.

Nel redigere il presente documento si è altresì tenuto conto del c.d. Decreto di armonizzazione d. rgs. 10//08/2018, n.101, con il quale sono state portare modificazioni ed integrazioni al Decreto Legislativo 30/06/2003 n.196, il quale, così novellato, continua a costituire la normativa Nazionale di riferimento in materia di trattamento dei dati personali, ad integrazione dei principi generali Comunitari di cui al citato GDPR.

Il presente documento definisce i criteri organizzativi, procedurali e tecnologici per la gestione della sicurezza in merito al trattamento dei dati personali, sensibili e/o giudiziari, le figure chiave della privacy previste dalla normativa e formalità per l'attribuzione di compiti/incarichi particolari. Vengono identificate le misure di natura organizzativa e tecnologica atte a garantire il raggiungimento ed il mantenimento nel tempo, dei livelli di sicurezza ritenuti adeguati per la salvaguardia delle informazioni trattate e delle risorse gestite dalla società.

2 VALIDITÀ E DESTINATARI DEL DOCUMENTO

Il presente documento ha validità fino a che non insorgano importanti modifiche organizzative, tecniche, procedurali o legislative. In tali casi deve essere revisionato/implementato onde assicurare

un adeguato livello di sicurezza ai dati personali, rapportato alle differenti categorie di dati trattati, in relazione alle eventuali variazioni del livello di rischio a cui gli stessi sono soggetti e ad eventuali modifiche della tecnologia informatica utilizzata dall'organizzazione.

Il Documento si applica a tutto il personale ed ai collaboratori esterni di Ser.In.Ar., in particolare alle funzioni aziendali incaricate di progettare ed aggiornare il piano di protezione del sistema informativo/cartaceo e di effettuare i relativi controlli.

Per i fornitori di servizi esterni all'organizzazione della Società è il Titolare autonomo/Responsabile del trattamento dei dati che richiede al proprio personale il rispetto delle disposizioni loro riguardanti.

Per quanto riguarda i dati trattati da Ser.In.Ar per conto degli Enti che la partecipano, si provvederà di volta in volta in relazione alle specifiche attività richieste, a formalizzare mediante apposito contratto eventuali rapporti di contitolarità o di semplice incarico di Responsabile Esterno in conformità al GDPR.

3 DEFINIZIONI

Si richiama integralmente il contenuto di cui all'art. 4 del GDPR 2016/679/UE concernente la definizione dei significati attribuiti alle locuzioni rilevanti ai fini dell'esatta comprensione della normativa, precisandosi che per quanto non specificato nella presente sezione "definizioni" deve farsi riferimento a detta richiamata norma.

Qui di seguito si riportano, pertanto, solo le definizioni maggiormente rilevanti ai predetti fini, nonché le definizioni aggiuntive ritenute utili per la migliore comprensione del presente regolamento.

Titolare del trattamento dei dati: 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 di dati personali;

Responsabile del trattamento dei dati: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

Incaricato del trattamento dei dati: la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile

D.P.O. (o R.P.D.): il responsabile della protezione dei dati designato, ai sensi dell'articolo 37 del GDPR, dal Titolare del trattamento e/o dal Responsabile del trattamento, al quale viene affidata la sorveglianza circa l'osservanza del presente regolamento e delle disposizioni normative dell'unione e dello Stato Italiano, al quale vengono attribuite le prerogative ed assegnati i compiti di cui agli articoli 38 e 39 del GDPR

Interessato: la persona fisica identificata o identificabile a seguito della raccolta dei dati; si precisa che alle persone giuridiche non è attribuibile la qualità di interessato

Amministratore di Sistema:figura professionale è finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti e/o amministratore di basi di dati, di reti e di apparati di sicurezza e/o di sistemi software complessi

Dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati particolari: i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

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

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Dati giudiziari: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza

Dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile, può essere trattato senza il consenso da parte dell'interessato.**(pseudonimizzazione)**

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione

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

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

Banca di dati: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Misure di sicurezza: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione adottato dal Titolare del trattamento, dal Responsabile del trattamento, o suggerito dal D.P.O.

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico, ed indipendentemente che sia costituito in formato cartaceo o informatizzato ho in entrambe le predette modalità

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile

Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento, l'insieme degli strumenti elettronici e delle procedure per la verifica dell'identità o della dichiarazione di identità

Sistemi di videosorveglianza: i sistemi elettronici per la visione di immagini attraverso strumenti di ripresa sia fissi che con la possibilità di "zoom", con la possibilità di registrare tali immagini per il tempo previsto dalla vigente normativa e dalle disposizioni dell'Autorità di Controllo

Credenziali di autenticazione: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati dal sistema di autenticazione informatica per la verifica dell'identità o di una dichiarazione di identità

Parola chiave: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica

Profilo di autorizzazione: l'insieme dei dati cui una persona può accedere, nonché dei trattamenti ad essa consentiti

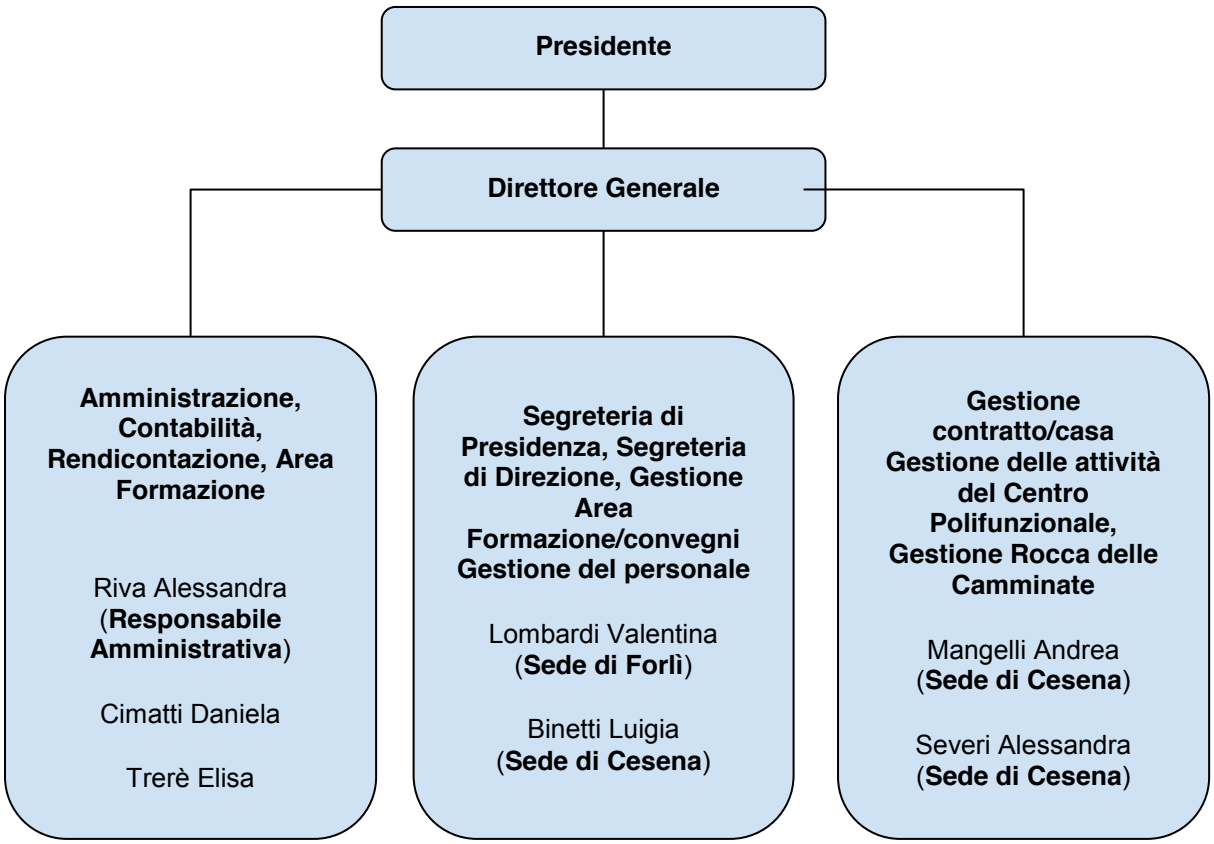
Sistema di autorizzazione:l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente

Cookies: stringhe di testo di piccole dimensioni che i siti visitati dall'utente inviano al suo terminale (solitamente al browser), dove vengono memorizzati per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo utente.

4 DESCRIZIONE DI SER.IN.AR.

4.1 Struttura organizzazione interna

Ser.In. Ar. agisce sulla base di una pianta organica ben definita e così composta:



- *Fabrizio Abbondanza – Direttore Generale*
- *Alessandra Riva – Responsabile Amministrativo*
- *Daniela Cimatti - Ragioniera*
- *Treré Elisa - -Ragioniera*
- *Valentina Lombardi- Segretaria di presidenza e Direzione*
- *Luigia Binetti – Impiegata con funzioni di Segretario*
- *Andrea Mangelli – Impiegato d'ordine*
- *Alessandra Severi - Impiegata d'ordine*

4.2 Politiche aziendali

SER.IN.AR., pur avendo dedicato particolare attenzione al tema del corretto trattamento dei dati personali, sia in sede di gap analisys sia in sede di conseguente approntamento delle misure di sicurezza ritenute idonee a prevenire possibilità di illecito o non conforme trattamento, è perfettamente consapevole che il margine di rischio non può essere azzerato ma solo congruamente ridotto in sede di analisi prognostica, il che tuttavia lascia un margine residuo di possibili inconvenienti e correlate azioni risarcitorie e/o sanzionatorie.

Ciò premesso Ser.In.Ar ha ritenuto opportuno, in un'ottica di responsabile e consapevole gestione delle risorse pubbliche ad essa conferite, prevedere un progressivo accantonamento annuale, in caso di avanzo di gestione, atto a garantire alla stessa una disponibilità economica in ipotesi in cui venga chiamata a rispondere, a fronte di eventuali responsabilità, sia da parte dell'autorità di controllo sia da parte di terzi. Tale accantonamento verrà appostato in bilancio sotto il nome di "Accantonamento privacy".

Ser.In.Ar., inoltre, si riserva di verificare sul mercato assicurativo l'offerta di prodotti intesi a coprire il sopra evidenziato rischio; laddove tali coperture saranno possibili e compatibili con le risorse aziendali, SER.IN.AR. provvederà ad accendere le relative polizze, e a liberare gli eventuali accantonamenti nel frattempo effettuati.

5 RUOLI E RESPONSABILITÀ PER IL TRATTAMENTO DEI DATI PERSONALI

Il "Codice in materia di protezione dei dati" (GDPR 2016/679/UE) individua alcune "figure chiave" soggettive cui sono attribuiti specifici obblighi e diritti in relazione all'attività di trattamento dei dati personali.

Ser.In.Ar in ossequio alla normativa di riferimento, ha adottato un "Funzionigramma Privacy" (allegato 1) nel quale sono illustrate le linee gerarchiche (funzionali e di staff) che fanno capo ai ruoli privacy istituiti all'interno di essa, unitamente alle figure che trattano banche dati sensibili (sorveglianza sanitaria e sicurezza sul lavoro), al fine di consentire il corretto assolvimento di tutti gli adempimenti previsti dal Codice, e di cui si riporta nel seguito una breve descrizione.

5.1 Titolare del Trattamento dei dati

Titolare del trattamento dei dati (Capo IV GDPR 2016/679/UE) è Ser.In.Ar., nel suo complesso, la cui rappresentanza legale nei confronti di terzi è statutariamente attribuita al Presidente Pro-Tempore.

I principali compiti del Titolare del trattamento dati sono quelli di mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Tali misure vengono decise dal C.d.A.; le spese necessarie alla regolare gestione della privacy trovano copertura in apposito capitolo del Bilancio.

Il Titolare del trattamento deve:

1. assumere tutte le decisioni in ordine alle finalità ed alle modalità del trattamento, ivi compreso il profilo della sicurezza;
2. procedere al censimento dei dati trattati ed all'individuazione della tipologia dei trattamenti effettuati sugli stessi ed effettuare, se necessario, la notificazione al Garante;
3. procedere all'individuazione ed alla nomina scritta dei Responsabili interni ed esterni del trattamento, all'individuazione degli eventuali incaricati del trattamento;
4. provvedere alla nomina del D.P.O., qualora necessario;
5. assicurarsi che il D.P.O. eserciti efficacemente la propria attività di vigilanza, anche tramite verifiche periodiche, sulla puntuale osservanza da parte degli Incaricati delle istruzioni impartite e delle vigenti disposizioni in materia di trattamento dei dati;
6. assicurarsi che il D.P.O. eserciti periodicamente la propria attività di vigilanza sulle attività degli Amministratori di sistema, attraverso gli *access log file* disponibili o altre metodiche di garanzia;
7. attuare gli obblighi di informazione ed acquisizione del consenso, quando richiesto, nei confronti dell'interessato;
8. adottare tutte le misure di sicurezza idonee per il trattamento dei dati sulla base di un criterio di responsabilità e di responsabilizzazione dei vari attori della privacy aziendale (Accountability);
9. garantire a tutti gli incaricati la corretta informazione e formazione sul tema della privacy e delle sue applicazioni in Ser.In.Ar.,mediante l'organizzazione di appositi eventi info-formativi;
10. redigere il Regolamento sulla Sicurezza e provvedere periodicamente al suo aggiornamento;
11. riferire all'Assemblea dei Soci nella relazione accompagnatoria del bilancio d'esercizio, dell'avvenuta redazione o aggiornamento del presente Regolamento.
12. nel caso di affidamento all'esterno di alcune attività di trattamento dei dati deve anche, avvalendosi del/dei Responsabile/i esterno/i del trattamento dei dati:
    a) valutare la posizione del soggetto esterno;

b) verificare i contratti che disciplinano l'affidamento all'esterno dei servizi connessi al trattamento dei dati, valutandone la compatibilità e la congruenza con il GDPR 2016/679/UE;

c) provvedere a formalizzare per iscritto tutte le istruzioni ed i compiti;

d) provvedere, qualora ne ricorrano i presupposti, dichiarare la contitolarità del trattamento, definendo congiuntamente con il contitolare le finalità ed i mezzi del trattamento, in conformità a quanto stabilito dall'art. 26 del GDPR 2016/679/UE

5.2 Responsabile del trattamento dei dati

5.2.1. Responsabile interno del trattamento dei dati

Nella struttura organizzativa interna di Ser.In.Ar., il ruolo di Responsabile interno del trattamento dei dati (art. 28 del GDPR 2016/679/UE) è ricoperto dal Direttore Generale in qualità di referente per la privacy.

Per la sicurezza sul lavoro dei lavoratori tale ruolo è ricoperto dal responsabile del servizio di prevenzione e protezione – RSPP, individuato con apposito incarico.

I principali compiti del Responsabile interno del trattamento sono:

1. provvedere alla predisposizione ed alla tenuta del registro trattamento dati, di cui all'art. 30 del GDPR 2016/679/UE, conformandolo alle indicazioni ivi previste al primo e secondo comma; al riguardo si evidenzia che Ser.In.Ar. è un'azienda pubblica con un numero di dipendenti largamente inferiore ai 250; pertanto si ritiene di unificare in un unico documento, a cura del Responsabile del Trattamento, le previsioni previste al primo e secondo comma di detto art. 30;
2. informare prontamente il Titolare di ogni questione rilevante ai fini della protezione dei dati personali/sensibili;
3. curare il coordinamento di tutte le operazioni di trattamento dei dati personali/sensibili sulla base delle istruzioni scritte impartite dal Titolare;
4. operare in sinergia con il Titolare per l'attuazione degli obblighi di informazione ed acquisizione del consenso, quando richiesto, nei confronti dell'interessato;
5. procedere alla nomina scritta degli Incaricati del trattamento dei dati e fornire loro il codice identificativo e la credenziale di autenticazione ed idonee istruzioni scritte in ordine alle modalità di trattamento;

6. promuovere lo svolgimento di un continuo programma di informazione/formazione e addestramento degli Incaricati del trattamento e mantenere attivo un programma di controllo e monitoraggio della corrispondenza con le regole di sicurezza;
7. gestire e coordinare tutte le attività legate alla sicurezza sia dei soggetti interni, sia degli eventuali soggetti esterni (*outsourcer*);
8. operare per l'effettuazione delle verifiche del livello di conformità riguardo a tutti gli adempimenti organizzativi, procedurali e di sicurezza previsti dal GDPR 2016/679/UE e relazionarne al Titolare;
9. per quanto attiene l'assolvimento degli obblighi generali di sicurezza, annualmente individuare/aggiornare le misure preventive e protettive atte alla eliminazione/diminuzione dei rischi identificati, sottoporne l'elenco al Titolare e, in base alle sue indicazioni, predisporre il programma di attuazione particolareggiato di tali misure;
10. operare in sinergia con il Titolare per l'aggiornamento del Registro del Trattamento e del Regolamento Privacy sulla sicurezza dei dati;
11. verificare, nel caso di affidamento delle attività di trattamento a soggetti giuridici esterni, i contratti che disciplinano l'outsourcing, valutandone la compatibilità e la congruenza con il GDPR 2016/679/UE;
12. adottare le misure idonee a consentire all'Interessato l'effettivo esercizio dei diritti previsti dall'art. 12 del GDPR 2016/679/UE, e garantire detto esercizio;
13. evadere senza ritardo le eventuali richieste avanzate dagli interessati ai sensi dell'art. 15 del GDPR 2016/679/UE;

5.2.2. Responsabile esterno del trattamento dei dati

Ser.In.Ar. provvederà, all'occorrenza, a nominare eventuali responsabili esterni del trattamento dati in relazione alle necessità che si presenteranno, avendo riguardo alle modalità di trattamento dei dati stessi.

Tali eventuali nomine consisteranno in appositi incarichi/contratti scritti.

5.3 Incaricati del Trattamento dei dati

Incaricati del trattamento dei dati sono tutti i collaboratori interni ed esterni e i dipendenti che abbiano accesso ai dati personali di qualunque categoria (ordinari, particolari, giudiziari) in forma cartacea o informatica.

L'incarico è affidato per iscritto dal Responsabile interno del trattamento dei dati mediante lettera di nomina che individua puntualmente l'ambito del trattamento consentito dei dati e fornisce loro il

codice identificativo e la credenziale di autenticazione ed idonee istruzioni scritte in ordine alle modalità di trattamento;

Ciascun Incaricato opera con responsabilità propria, rispettando le prescrizioni emesse dal Responsabile interno del Trattamento dati assumendo, in ordine al trattamento dei dati, le seguenti responsabilità:

1) svolgere le attività previste dai trattamenti attenendosi strettamente alle istruzioni impartite dal Responsabile interno del Trattamento dati ed alle prescrizioni di sicurezza contenute nel Documento di Analisi sulla Sicurezza dei dati;
2) non effettuare attività di trattamenti non consentite o non previste nell'ambito del suo ruolo aziendale senza l'esplicita autorizzazione del Responsabile interno del trattamento;
3) usare la massima riservatezza e discrezione durante le operazioni di trattamento dei dati e nella conseguente loro protezione;
4) rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
5) evitare i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta, in armonia con gli obblighi derivanti dal regolamento 2016/679/UE;
6) informare il Responsabile interno Trattamento dati in caso di diminuzione del livello di sicurezza che coinvolga dati personali.

5.4 Amministratori di sistema

Viene definito quale "amministratore di sistema" colui che, in ambito informatico, ha una competenza professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti e/o amministratore di basi di dati, di reti e di apparati di sicurezza e/o di sistemi software complessi.

L'Amministratore di sistema, pur non essendo preposto ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), svolge, nella Sua consueta attività, in molti casi, specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

L'Amministratore di sistema" ha il compito di:

1. interfacciarsi con il Responsabile interno per quanto riguarda l'implementazione/aggiornamento delle politiche e delle procedure di sicurezza previste per la gestione dei sistemi informativi;
2. assicurare la corretta applicazione delle politiche, procedure e standard di sicurezza predisposte per la manutenzione hardware e software;
3. consentire all'Incaricato l'autonoma modifica della parola chiave al primo utilizzo del software di gestione della banca dati, ove ciò sia tecnicamente possibile, e successivamente almeno ogni sei mesi, nel caso di trattamento di dati personali, e almeno ogni tre mesi, nel caso di trattamento di dati sensibili e di dati giudiziari;
4. disattivare le credenziali di autenticazione non utilizzate da almeno sei mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica, in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali;
5. configurare i profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sulla base delle indicazioni fornite dal Responsabile del trattamento dei dati ed in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento;
6. periodicamente, e comunque almeno annualmente, verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione;
7. proteggere i dati personali e gli elaboratori utilizzati per il trattamento degli stessi contro il rischio di intrusione e dell'azione di *malicious program*, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale;
8. aggiornare periodicamente i programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici ea correggerne difetti;
9. definire in accordo con il Responsabile interno del trattamento la pianificazione delle attività atte a evitare violazioni interne o esterne;
10. effettuare il salvataggio dei dati sensibili e/o giudiziari,presenti sulle unità di storage centralizzate, con frequenza almeno settimanale e secondo le istruzioni organizzative e tecniche impartite dal Responsabile Interno del trattamento dei dati;
11. verificare l'integrità dei supporti di memorizzazione prima dell'utilizzo e procedere alla loro distruzione nel caso in cui non possano essere più riutilizzati;
12. proporre l'adeguamento dei sistemi (HW e SW) a livelli tecnologici tali da garantire la disponibilità del servizio;
13. prevedere e svolgere attività di controllo sull'operato di personale esterno a Ser.In.Ar. per interventi di installazione, aggiornamento e manutenzione HW e SW;
14. collaborare con il Responsabile interno del trattamento dei dati alla stesura/aggiornamento del Documento Programmatico sulla Sicurezza.

6 ANALISI DEL RISCHIO

Il Titolare del trattamento ha ritenuto opportuno adottare misure di sicurezza idonee a ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o trattamento dei dati personali non consentito o non conforme alle finalità della raccolta.

In particolare, il Titolare ha adottato le misure di sicurezza che ha ritenuto indispensabili a garantire un livello minimo di sicurezza per tutti i trattamenti in essere; ha adottato inoltre misure specifiche di maggiore garanzia in presenza di trattamento di eventuali dati particolari, nonché in presenza di aree di rischio maggiormente elevate.

Detta valutazione e le conseguenti misure sono riportate in apposita sezione del registro del trattamento dati (Allegato 4).

Appare necessario, dunque, identificare ed implementare le misure di sicurezza maggiormente idonee a garantire la protezione dei dati, ovvero quelle misure determinate in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento.

Tale valutazione non può prescindere da un'attività di Analisi dei Rischi volta a:

- § classificare i dati in base al loro livello di criticità/rischio;
- § analizzare le minacce e le vulnerabilità del sistema informativo;
- § identificare ed implementare le contromisure maggiormente idonee a garantire un livello di sicurezza adeguato per la protezione dei dati particolari di dati personali.

6.1 Metodologia utilizzata

In questa sezione vengono descritti i criteri adottati da Ser.In.Ar. nella conduzione dell'analisi di rischio, al fine di proteggere i dati personali sensibili e/o giudiziari.

Il livello di rischio si esprime come combinazione dei seguenti parametri:

- la gravità delle conseguenze di eventi, espressa in termini di impatti tangibili o intangibili;
- la relativa probabilità stimata di accadimento, determinata su base annuale,

come nell'immagine di seguito riportata:

P = Probabilità di accadimento

G = Gravità delle conseguenze

R = Livello di rischio = P x G

Nella rappresentazione dei rischi, i livelli di probabilità e gravità possono essere assegnati su base storica o su valutazioni di natura prevalentemente qualitativa o, qualora siano disponibili idonei dati statistici, in forma quantitativa, con riferimento alla schematizzazione riportata nelle successive tabelle 1 e 2.

Convenzionalmente le probabilità e gravità dei rischi, vengono assegnati in base a scale per numeri interi variabili da 0 a 3.

Tabella 1: attribuzione delle classi di probabilità dei rischi

Punteggio	Livello	Descrizione
3	**Alto**	Probabilità di accadimento dell'evento considerata stimata superiore a 5 casi su base annuale.
2	**Medio**	Probabilità di accadimento dell'evento considerata stimata tra i 3 e i 5 casi, su base annuale.
1	**Basso**	Probabilità di accadimento dell'evento considerata stimata in 1 evento su base annuale.
0	**Nullo o trascurabile**	Probabilità di accadimento dell'evento considerata stimata in 0 eventi su base annuale.

Tabella 2: attribuzione della gravità dell'impatto dei rischi

Punteggio	Gravità dell'impatto	Descrizione
3	**Molto critica**	Gravi impatti o conseguenze gravi
2	**Significativa**	Impatti significativi
1	**Bassa**	Impatti limitati
0	**Nulla o trascurabile**	Impatto nullo o trascurabile

Le classi di rischio risultanti, sono rappresentati nella tabella 3.

Tabella 3: Classificazione degli indici di rischio

Indice di rischio	Classificazione degli indici di rischio e delle azioni suggerite	
R > 6	**Alto**	È una condizione non accettabile, per la quale è richiesta una sensibilizzazione al più alto livello di management coinvolto, un rafforzamento delle azioni di prevenzione e protezione in essere nel sistema di gestione, un'adeguata destinazione di risorse destinate al controllo della efficace attuazione delle misure adottate.
3 < R ≤ 6	**Medio**	È una condizione non accettabile, che richiede una sensibilizzazione a livelli appropriati del Coordinatore Generale, un adeguamento delle azioni di prevenzione e protezione in essere nel sistema di gestione,

1 ≤ R ≤ 3	**Basso**	È una condizione accettabile, in quanto richiede una sostanziale conferma delle misure organizzative già previste nel sistema di gestione, integrata al più da una sensibilizzazione del Coordinatore Generale e dal monitoraggio delle relative attività.
R = 0	**Nullo o trascurabile**	Rischio trascurabile o nullo: non richiede alcuna azione.

6.2 Risultati dell'attività

Lo svolgimento dell'attività di analisi dei rischi ha condotto Ser.In.Ar. all'identificazione del livello di rischio calcolato su una scala di valori stimata in Alto, Medio, Basso, Nullo o trascurabile, cui i beni sono potenzialmente esposti.
A tal fine, Ser.In.Ar. ha effettuato un check up delle proprie banche dati, provvedendo contestualmente ad individuarne:

- La tipologia di banca dati;
- L'ufficio/funzione ove sono allocate;
- La tipologia di dati contenuti (Dati Particolari o Ordinari);
- Il tipo di formato (cartaceo, elettronico);
- I programmi utilizzati per la loro elaborazione;
- Le locazioni ove fisicamente sono ubicate le macchine;
- Il livello di rischio;
- Le misure adottate per ridurre o eliminare il rischio,
- Categoria degli interessati,
- Destinatari,
- Durata massima del trattamento.

Gli esiti dell'analisi sono stati riportati nel "Registro del Trattamento", oggetto di verifica ed aggiornamento annuale.

7 MISURE DI SICUREZZA CONTRO IL RISCHIO DI DISTRUZIONE/PERDITA DEI DATI (D.P.I.A.)

A seguito della redazione e stipulazione di apposita convenzione con Unibo, ad oggi in fase di elaborazione, in questa sezione verranno descritte le contromisure di sicurezza fisiche, logiche ed organizzative adottate da Ser.In.Ar. per fronteggiare il rischio di distruzione/perdita dei dati trattati.

7.1 Misure di sicurezza contro il rischio di distruzione da incendio

Sede legale: Ser.In.Ar.ha predisposto un idoneo Piano di emergenza secondo la normativa specifica in ambito di prevenzione incendi. Nella sede sono affisse le planimetrie di emergenza ed è stato redatto il piano di emergenza e le norme comportamentali da tenere in caso di emergenza.

Sede Operativa : E' stato predisposto un apposito Documento di valutazione dei rischi per la salute e la sicurezza soggetto a periodico aggiornamento in caso di variazioni rilevanti.

8 MISURE DI SICUREZZA CONTRO IL RISCHIO DI ACCESSO NON AUTORIZZATO

In questa sezione, vengono riportate le misure di sicurezza definite da Ser.In.Ar., sia per la sede di Forlì che per la sede di Cesena, sulla base dei dettami del Codice e dei risultati dell'attività di analisi dei rischi, per fronteggiare i rischi di accesso non autorizzato alle informazioni.

Questa sezione verrà aggiornata a seguito della stipulazione dell'apposita convenzione in redazione con Unibo.

8.1 Protezione delle aree e dei locali

Per l'accesso alla sede di Ser.In.Ar è necessario qualificarsi.

Le stanze degli uffici sono protette da porte dotate di chiave. Armadi e cassettiere presenti all'interno degli uffici sono dotati in gran parte di alloggiamenti dotati di chiusura a chiave nei quali archiviare i documenti più riservati. La custodia di tali chiavi è affidata al singolo dipendente.

8.2 Utilizzo e riutilizzo dei supporti di memorizzazione

I supporti rimovibili contenenti dati sensibili e/o giudiziari possono essere riutilizzati da altri Incaricati, non autorizzati al trattamento degli stessi dati, solo se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

I supporti rimovibili contenenti dati sensibili e/o giudiziari se non utilizzati sono distrutti o resi inutilizzabili

Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati (vedi documento "Istruzioni per gli Incaricati")

9 MISURE DI SICUREZZA CONTRO IL RISCHIO DI TRATTAMENTO NON CONSENTITO E/O NON CONFORME

In questa sezione vengono riportati i criteri definiti dall'organizzazione sulla base dei dettami del Codice e dei risultati dell'attività di analisi dei rischi, per fronteggiare i rischi di trattamento non consentito; il presente paragrafo verrà integrato in conformità all'adottanda convenzione con Unibo.

9.1 Personale autorizzato al trattamento dei dati

La designazione degli Incaricati è effettuata per iscritto e deve individuare puntualmente l'ambito del trattamento consentito.

In caso di dimissioni di un Incaricato del trattamento o di revoca delle autorizzazioni al trattamento dei dati, il Responsabile del trattamento dei dati deve darne immediata comunicazione all'Amministratore di sistema di competenza che provvederà a disattivare la possibilità di accesso al sistema per il soggetto in questione.

Sono impartite, dal Responsabile all'Incaricato, istruzioni operative per il trattamento dei dati e istruzioni tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare trattamenti non consentiti dei dati.

9.2 Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni

L'Amministratore di sistema verifica annualmente le autorizzazioni di accesso alle banche dati oggetto del trattamento e se necessario, provvede a variare i profili di autorizzazione, confrontandosi sempre con il Responsabile del trattamento.

10 MISURA PER IL RISCHIO DI INDISPONIBILITÀ DEI DATI

In questa sezione vengono descritti i criteri e le modalità per il ripristino della disponibilità dei dati a seguito di distruzione o danneggiamento, definite da Ser.In.Ar. sulla base dei dettami del Codice e dei risultati dell'attività di analisi dei rischi; la presente sezione verrà aggiornata in conformità con l'adottanda convenzione con Unibo.

10.1 Criteri per il ripristino dei dati

Nel caso di trattamento di dati devono essere adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici.

Nel caso di trattamento di dati particolari il ripristino deve avvenire in tempi certi compatibili con i diritti degli interessati.

10.2 Danneggiamento dell'hardware

Nell'eventualità che si danneggino in modo disastroso uno o più componenti hardware di un Server, necessari al suo funzionamento, si interverrà tempestivamente per ripristinare i servizi nel più breve tempo possibile procedendo secondo le seguenti modalità:

- Eventuale spostamento temporaneo dei servizi non operativi su un altro Server, tenendo in considerazione i tempi e gli oneri di un tale intervento;
- Sostituzione immediata delle parti danneggiate se presenti in Azienda come parte di ricambio, oppure acquisto delle parti presso il produttore e invio delle stesse tramite corriere espresso;

Se il danno hardware riguarda le unità di memorizzazione di massa (hard disk) si intraprenderanno azioni specifiche, come definito nell'apposita convenzione con Unibo, in fase di elaborazione.

Nel caso in cui la non disponibilità dei servizi sia causa di malfunzionamenti software, è necessario:

- Ripristinare nel più breve tempo possibile i servizi isolando la causa del problema, valutando l'eventuale momentanea sospensione di altri sistemi in conflitto;
- Installare nuovamente o spostare su altri Server il servizio non disponibile, valutando costi ed oneri che tale attività implica.

10.3 Intrusioni nel sistema informatico

Si richiamano le misure di cui ai precedenti paragrafi 8 e 9, da integrarsi a seguito dell'apposita convenzione con Unibo, in fase di elaborazione.

10.4 Modalità di dismissione di hardware obsoleto

Se si rende necessario dismettere il disco rigido e/o memorie di massa di strumenti informatici che contenga o possa avere contenuto dati personali e/o sensibili e/o giudiziari, si adotteranno specifiche attività da concordarsi con l'amministratore di sistema.

10.5 Modalità di gestione degli account di posta per assenza dell'incaricato

In caso di eventuali assenze non programmate (es: per malattia), qualora il lavoratore non possa attivare la procedura sopra descritta, il Titolare del trattamento, perdurando l'assenza oltre 7 giorni, se

necessario e attraverso l'operato degli Amministratori di Sistema, dispone l'attivazione della sopra citata procedura, avvertito l'interessato.

Se un incaricato al trattamento dei dati dovesse rimanere assente dal lavoro improvvisamente o per un lungo periodo e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, viene consentita la possibilità di delegare a collega di fiducia o, se non possibile, consentito all'Amministratore di Sistema, a verificare il contenuto di messaggi e a inoltrare al Responsabile del trattamento, per conto del Titolare, quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa, informando il lavoratore alla prima occasione utile.

10.6 Modalità di gestione degli account di posta per dimissioni o licenziamento dell'incaricato

Dal ricevimento della comunicazione mail da parte dell'Ufficio Personale con i riferimenti del lavoratore dimesso o licenziato per giusta causa, gli Amministratori di Sistema provvedono a:

- impostare un risponditore automatico per consentire di inviare automaticamente messaggi di risposta contenenti le coordinate (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura.
- disabilitare l'account di posta entro due mesi dalla data delle dimissioni o del licenziamento.

10.7 Modalità di gestione dei documenti di lavoro

Relativamente ai file aziendali residenti sul PC o sul server gestiti dal lavoratore assente, dimesso o licenziato, il Responsabile del trattamento deciderà a quale altro incaricato assegnarne l'utilizzo.

11 SICUREZZA NELL'OUTSOURCING

In questa sezione, vengono descritti i criteri e le modalità per garantire l'adozione delle misure di sicurezza in caso di *outsourcing* delle attività di trattamenti di dati.

Il Titolare può decidere di affidare il trattamento di alcune banche dati (riguardanti ad es: elaborazione buste paga, servizio prevenzione e protezione, ecc.), a soggetti terzi esterni all'organizzazione di Ser.In.Ar. Questi ultimi, in virtù del contratto sottoscritto e delle condizioni contrattuali (privacy e riservatezza) in esso contenute, possono assumere la veste di Titolari autonomi, Contitolari o Responsabili esterni del trattamento.

Tali qualità verranno definite di volta in volta, in relazione ai singoli trattamenti affidati, sulla base delle corrispondenti lettere di incarico nelle quali verranno specificate i trattamenti o le parti di trattamento affidati.

Nell'Allegato 3 vengono indicati i soggetti in outsourcing con le corrispondenti funzioni di rispettiva competenza. Tali soggetti sono tenuti al rispetto autonomo del GDPR 2016/679/UE qualora Titolari o Contitolari; saranno tenuti al rispetto delle indicazioni di Ser.In.Ar qualora Responsabili esterni del trattamento.

Il Titolare autonomo ed il Contitolare del trattamento sono tenuti a comunicare a Ser.In.Ar. che sono state adottate le misure idonee di sicurezza per il trattamento dei dati di Ser.In.Ar. secondo quanto disposto dalla vigente normativa, e che il trattamento verrà effettuato in conformità alla stessa.

12 FORMAZIONE E SENSIBILIZZAZIONE

In questa sezione, vengono descritti i criteri e le modalità per svolgere l'attività di sensibilizzazione e informazione/formazione del personale di Ser.In. Ar., come previsto dalla normativa di riferimento.

12.1 Pianificazione degli interventi formativi

La formazione viene programmata al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi e significativi strumenti operativi, rilevanti rispetto al trattamento di dati personali.

Ser.In.Ar al fine di ottemperare a quanto stabilito dal GDPR pianifica annualmente il corso di formazione e sensibilizzazione in materia privacy, il cui scopo è quello di rendere edotto tutto il personale incaricato al trattamento di dati personali:

- § dei rischi che incombono sui dati;
- § delle misure disponibili per prevenire eventi dannosi;
- § dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività;
- § delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure di sicurezza adottate dal Titolare.

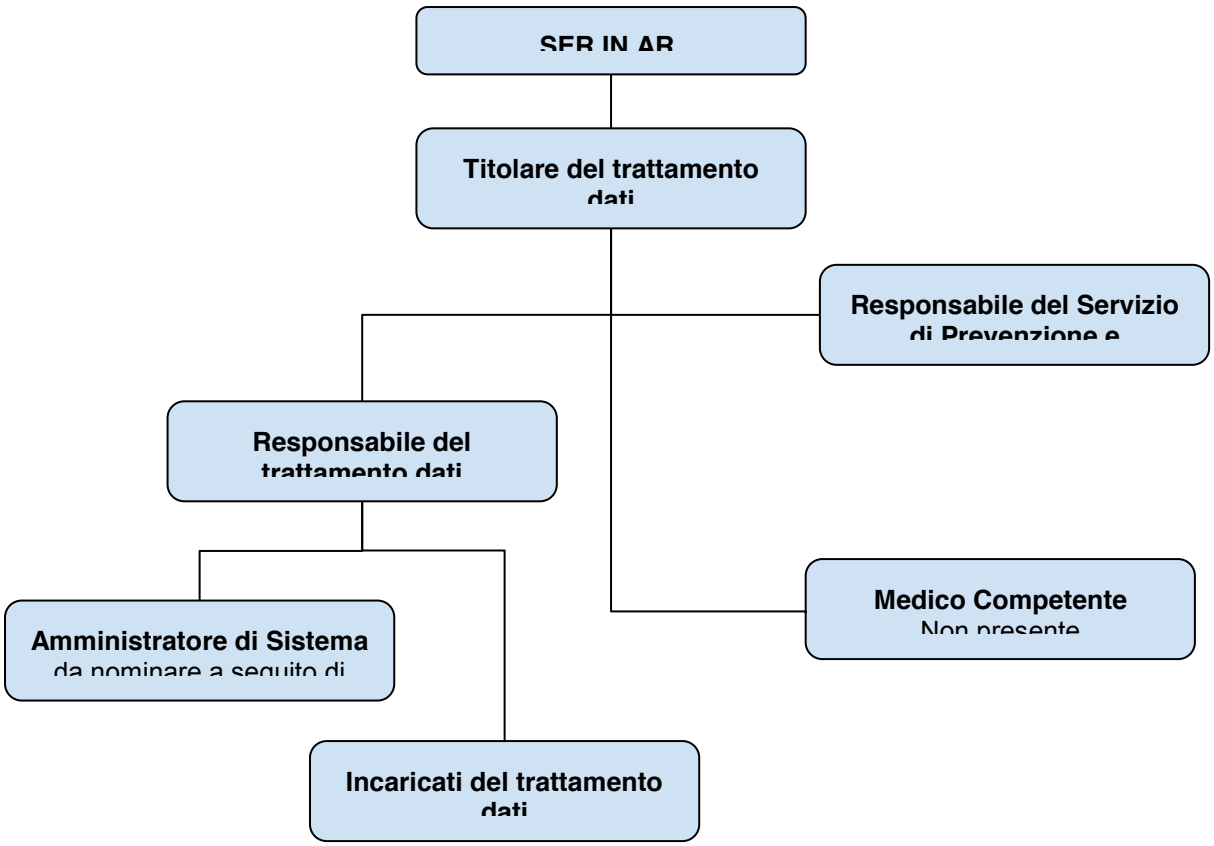
La progettazione del Piano di Formazione di Ser.In.Ar e la realizzazione degli interventi formativi in esso contenuti, contribuiscono a diffondere efficacemente le risultanze dell'attività di analisi dei rischi, le politiche e le procedure di sicurezza adottate dall'organizzazione, e le modalità di utilizzo corretto degli strumenti informatici, minimizzando la componente, sempre presente, di resistenza al cambiamento.

Forlì, _____

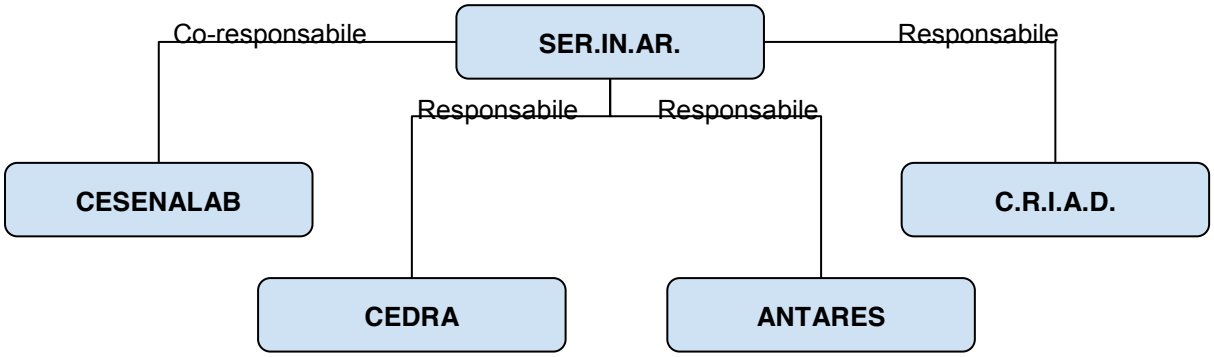
Il Titolare del trattamento dei dati –
Ser.In.Ar.

_____

ALLEGATO 1 – FUNZIONIGRAMMA PRIVACY



ALLEGATO 1A – SCHEMA DEI RAPPORTI DI CO-TITOLARITÀ - RESPONSABILITÀ DELLE STRUTTURE FACENTI CAPO A SER.IN.AR.



ALLEGATO 2– ELENCO DEGLI AMMINISTRATORI DI SISTEMA

Cognome	**Nome**	**Funzione aziendale**	**Software e Hardware gestiti**
da nominare a seguito di apposita convenzione con Unibo		Resp. Operativo Sviluppo Tecnologico	Tutti i sistemi installati e le banche dati operanti

ALLEGATO 3 – ELENCO DEGLI OUTSOURCER

Attività delegata	**Descrizione sintetica**	**Dati personali, sensibili o giudiziari interessati**	**Soggetto esterno**	**Delibere o atti di adozione**

Software Fatturazione Elettronica	Attività di fatturazione legata alla vendita di pacchetti formativi.	Dati personali e dati sensibili	Team System	
software gestionale di piattaforma CRM	Attività di gestione di piattaforma CRM	Dati personali	ASTER.S.Cons.p.a.	
Manutenzione software		Dati personali	in redazione convenzione con UNIBO	
Gestione PEC e email	Gestione e conservazione della Posta aziendale , compresa quella Certificata	Dati personali, sensibili e giudiziari	in redazione convenzione con UNIBO	
Gestione newsletters dell'Azienda	Gestione invio Newsletters	Dati personali	Grafikamente	
Servizio di prevenzione protezione per la Sicurezza sul Lavoro		Dati personali, sensibili e giudiziari	RSPP - Prosit Soc. Coop.	
Tenuta del bilancio e adempimenti fiscali		Dati Personali	Studio R&E commercialisti associati	

Consulenza fiscale e civilistica, invio telematico delle dichiarazioni societarie.				
Consulenza del lavoro e paghe Elaborazione buste paga e pratiche dipendenti, elaborazione parziale e trasmissione telematica del modello 770.		Dati personali (personale dipendente, collaboratori a progetto (parasubordinati). Buste paga,iscrizione INAIL, iscrizione INPS)	Studio Ballardini	
Pratiche Edilizie		Dati personali	Ufficio tecnico dei Campus di Forlì e Cesena	
Manutenzione software gestionale amministrativo	Attività di manutenzione del software di gestione amministrativa contabile	Dati personali	Team System	
Manutenzione software di registrazione agli eventi	Attività di manutenzione del software di gestione presenza agli eventi	Dati personali	in redazione convenzione con Unibo	

*(da compilare a cura dell'azienda e mantenere aggiornato annualmente) si veda la Legenda.

***Legenda: informazioni contenute nelle tabelle**

Attività esternalizzata: contiene il tipo di attività che è stata affidata/oggetto di delega a terzi esterni all'organizzazione di Ser.In.Ar.

Descrizione sintetica: contiene una descrizione sintetica dell'attività affidata/delegata.

Dati personali, sensibili o giudiziari interessati: contiene l'elenco dei dati personali, sensibili o giudiziari oggetto di trattamento per la realizzazione dell'attività affidata/delegata.

Soggetto esterno: riporta l'identificativo della società esterna o del consulente esterno a cui è stato affidato l'incarico.

Descrizione impegni assunti: affinché sia garantito un adeguato trattamento dei dati, è necessario che la società/consulente che viene delegata/delegato al trattamento dei dati, si assuma alcuni impegni definiti su base contrattuale. Essi sono riconducibili ai seguenti esempi (a titolo non esaustivo):

- Il Titolare/Responsabile dell'azienda a cui le attività sono affidate, dichiara di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali, sensibili o giudiziari e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
- Il Titolare/Responsabile dichiara di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
- Il Titolare/Responsabile accetta di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere;
- Il Titolare/Responsabile si impegna a relazionare periodicamente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
- Il Titolare/Responsabile riconosce il diritto del Committente (Ser.In.Ar.) a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

In questa casella sono riportati gli impegni contrattualmente assunti nel caso specifico (rimandando allo specifico contratto in essere tra le parti).

ALLEGATO 4

Approvato dal Consiglio di Amministrazione in data 15/03/2021

"CESENALAB - IDEE PER CRESCERE"

1) DEFINIZIONE

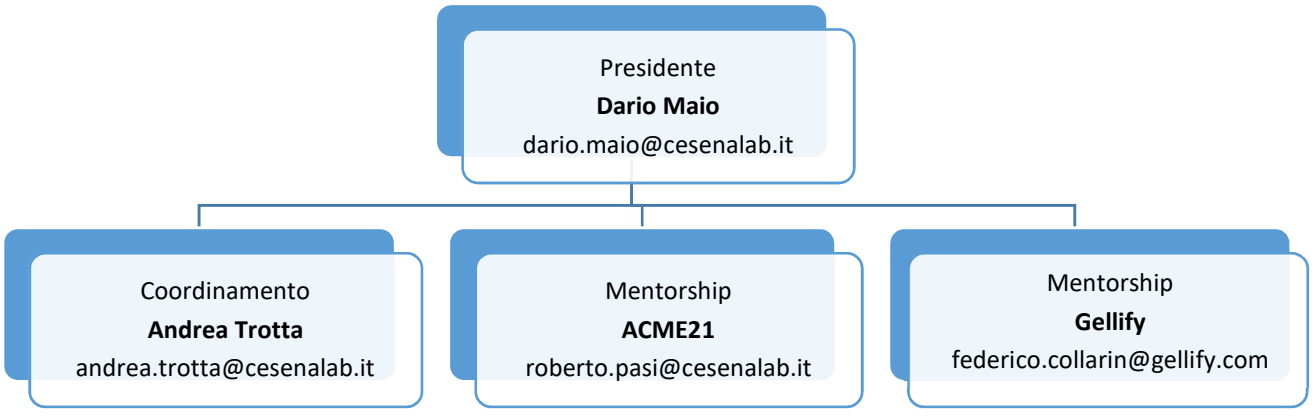
Cesenalab è un progetto nato dalla collaborazione tra il Comune di Cesena e numerosi Enti pubblici, privati e associazioni di categoria presenti sul territorio, con la finalità di avviare e sviluppare nuove imprese innovative nel settore informatico e tecnologico. L'incubatore e acceleratore d'impresa CesenaLab intende favorire il processo di sviluppo imprenditoriale dei team e delle startup selezionati in conformità all'Avviso pubblico "Invito a presentare progetti finalizzati all'inserimento nell'incubatore d'impresa CesenaLab – Idee per crescere", incentivandone la crescita e mettendo a disposizione delle stesse locali e servizi.

Con verbale del Consiglio di Amministrazione di Ser.In.Ar Forlì-Cesena Soc. Cons.p.A., redatto per atto pubblico a rogito del Notaio De Simone Rep. n. 54476 del 26.09.2018, raccolta 29109, registrato a Forlì il 28.09.2018 n. 6899 serie 1T, è stata approvata la costituzione di un patrimonio destinato ad uno specifico affare, ai sensi e per gli effetti dell'art. 2447 bis c.c., denominato CESENALAB, a far data dal 01.01.2019 con termine al 31.12.2021.

La gestione degli aspetti logistici, delle attività funzionali, delle attività di promozione delle start up e quanto necessario alla realizzazione delle finalità previste dall'incubatore Cesenalab – Idee per Crescere è demandato a Ser.In.Ar., come da specifico accordo con il Comune di Cesena, sottoscritto in data 3/12/2018, finalizzato all'avviamento e allo sviluppo di nuove imprese innovative nel settore informatico e tecnologico per il triennio 2019-2021.

2) STRUTTURA ORGANIZZATIVA INTERNA

CesenaLab agisce sulla base di una pianta organica così definita:



La sede di CesenaLab è sita nei locali ubicati in via Martiri della Libertà 14/C, Cesena, in comodato d'uso gratuito concesso dal Comune di Cesena, nel quale è collocata l'attrezzatura hardware e software necessaria per la realizzazione del progetto.

3) VIDEOSORVEGLIANZA

A seguito della necessità di tutelare l'area dedicata alla realizzazione dei progetti, che può essere sottoposta a rischi di perdita di valore e/o distruzione per atto vandalico, evento calamitoso e/o malavitoso/furti, si è ritenuto necessario ed opportuno addivenire alla sistemazione e funzionamento di un servizio di videosorveglianza nei locali siti in via Martiri della Libertà 14, Cesena, definito mediante l'apposizione di telecamere, come di seguito descritto.

Nell'immobile sono presenti n° 2 telecamere, una posizionata al piano terra ed una posizionata al primo piano. Le telecamere sono di tipo fisso e riprendono le immagini 24h senza effettuare registrazioni.

Alla chiusura degli uffici viene attivato un sistema di sorveglianza che monitora gli accessi. In caso di attivazione dell'allarme, le due telecamere registrano le immagini all'interno di una memoria (SD Card) collocata nelle telecamere stesse. I video registrati in seguito a tali eventi rimangono nelle memorie delle telecamere fino alla loro messa a disposizione dell'Autorità Giudiziaria o P.G.

L'impianto è predisposto per l'accesso da remoto mediante collegamento ad Internet attraverso un computer portatile ed uno smartphone in dotazione al Responsabile al Coordinamento, le credenziali per l'accesso al sistema, la gestione delle registrazioni e dell'allarme sono a disposizione del Responsabile e di un ulteriore soggetto all'uopo autorizzato.

4) BADGE DI ACCESSO AI LOCALI

Per poter accedere ai locali di lavoro riservati alle startup presso la sede dell'incubatore Cesenalab in via Martiri della Libertà n. 14/C, i membri delle startup ed i soggetti interessati sono dotati di badge di accesso, rilasciato previa compilazione di apposita modulistica.

L'utilizzo dei badges e i dati degli accessi vengono registrati mediante apposito programma, installato nel computer in dotazione al Responsabile del coordinamento, le credenziali sono a disposizione del Responsabile e di un ulteriore soggetto all'uopo autorizzato.