SERCOP

AZIENDA SPECIALE
DEI COMUNI DEL RHODENSE
PER I SERVIZI ALLA PERSONA

Regolamento sulle misure di sicurezza per il trattamento dei dati personali ex art. 32 Reg. UE 679/2016 (GDPR)

Approvato con Del. nr. xx del CdA del 28/12/ 2022

INDICE GENERALE

1. SCOPO E APPLICABILITÀ

Il presente documento costituisce parte integrante del registro delle attività di trattamento adottato dall'AZIENDA SPECIALE CONSORTILE SER.CO.P (Azienda Servizi Comunali alla Persona) con sede in Via Cornaggia, 33 a Rho (MI), ai sensi dell'art. 30, c. 1, lett. g) del Reg. UE n. 679/2016 (GDPR), e fornisce una descrizione generale delle misure tecniche ed organizzative che SER.CO.P. adotta al fine della tutela dei dati personali trattati dall'organizzazione, per garantire un livello di sicurezza ritenuto adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento.

Il presente documento annulla e sostituisce integralmente il documento "*DOCUMENTO PROGRAMMATICO SULLA SICUREZZA ", precedentemente adottato dall'Azienda.*

2. DEFINIZIONI ED ABBREVIAZIONI

Si riportano di seguito alcune definizioni utili per delineare il modello organizzativo e le misure adottate a tutela dei dati personali.

***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;

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

***Dati personali relativi a condanne penali e reati*:** 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;

***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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

***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;

***Responsabile interno del trattamento dei dati (o delegato al trattamento)*:** la persona fisica autorizzata dal Titolare a sovrintendere, con autonomia operativa, alle procedure del trattamento dei dati personali di un'unità organizzativa, o dell'Azienda nel suo complesso, garantendo il pieno rispetto e l'applicazione delle disposizioni normative e delle procedure aziendali vigenti in materia.

Referente privacy: la persona fisica che, all'interno dell'Azienda è incaricata di seguire operativamente le policy di privacy, propone la stesura dei regolamenti, delle procedure e della modulistica sulla privacy e sul trattamento dati ed effettua e valuta controlli sugli stessi.

***Incaricato al trattamento dei dati*:** la persona fisica autorizzata, dal Titolare o dal Responsabile interno, a compiere operazioni di trattamento di dati personali.

***Responsabile per la protezione dei dati (RPD/DPO)*:** soggetto a cui compete la vigilanza sull'osservanza del GDPR da parte del titolare del trattamento, mediante lo svolgimento di funzioni, previste dall'art. 39 del GDPR, di:

a) informazione e consulenza in merito agli obblighi derivanti dal GDPR e dalle altre normative in materia di protezione dei dati;
b) vigilanza sulla corretta attuazione del GDPR, delle altre disposizioni normative in materia e delle politiche adottate dal Titolare;
c) parere, se richiesto, in merito alla valutazione d'impatto sulla protezione dei dati e sorveglianza sul suo svolgimento ai sensi dell'articolo 35;
d) cooperazione con l'autorità di controllo (Garante) per questioni connesse al trattamento.

***Amministratore di sistema*:** Soggetto che, pur non essendo preposto ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle proprie consuete attività è, in molti casi, concretamente responsabile di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati personali. Rientrano in questa definizione figure professionali dedicate alla gestione e alla manutenzione di un impianto informatico di elaborazione dei dati o di sue componenti, nonché gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

3. RIFERIMENTI

3.1 Moduli

- Lettera di nomina Responsabile interno del Trattamento dei Dati
- Lettera di nomina Incaricato al Trattamento dei Dati
- Schema di accordo per la nomina del Responsabile del trattamento ex art. 28 GDPR;
- Regole generali interne per il trattamento dei dati personali
- Informative privacy per le diverse tipologie di interessati.

4. DESCRIZIONE DEL PROCESSO

4.1 Obiettivi

- Definire modalità operative e responsabilità per la gestione dei processi di emersione, analisi, correzione e miglioramento legati alle problematiche individuate che influenzino il servizio svolto;
- Definire modalità di comunicazione che consentano l'efficace conoscenza delle informazioni necessarie per la risoluzione delle specifiche problematiche e per prevenirne il ripetersi.

4.2 Responsabilità

***Titolare del trattamento*:** Titolare del trattamento dei dati personali è dall'AZIENDA SPECIALE CONSORTILE SER.CO.P (Azienda Servizi Comunali alla Persona) con sede in Via Cornaggia, n.33 a Rho (MI), rappresentata dal Presidente pro-tempore.

***Responsabile interno del trattamento (o delegato al trattamento)*:** Sono Responsabili interni del trattamento il Direttore generale e i Dirigenti delle Direzioni in cui è articolata l'Azienda. Al Responsabile Interno del trattamento sono attribuite le seguenti funzioni:

a) individua gli Incaricati del Trattamento dei dati, attraverso un atto di nomina individuale, corredato da strumenti idonei a impartire istruzioni e indicazioni pertinenti ed efficaci a garantire il rispetto della normativa in materia e della regolamentazione interna, con particolare riferimento al presente documento di "*Descrizione generale delle misure di sicurezza per il trattamento dei dati personali ex art. 32 Reg. UE 679/2016 (GDPR)*";
b) vigila circa il rispetto delle istruzioni specifiche impartite a tutti gli Incaricati del Trattamento dei dati personali e particolari;
c) identifica e censisce i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;
d) predispone il registro delle attività di trattamento da esibire in caso di ispezioni delle Autorità;
e) definisce, per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o rendere anonimi i dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
f) ogniqualvolta si raccolgano dati personali, provvede, tramite gli incaricati al trattamento, a che venga fornita l'informativa ai soggetti interessati;

g) assicura che la comunicazione a terzi e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali;
h) adempie agli obblighi di sicurezza, quali:
    a. adottare, tramite il supporto delle figure appositamente designate dall'Azienda, tutte le preventive misure di sicurezza, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
    b. definire una politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti al trattamento dei dati;
    c. assicurarsi la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
    d. testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;
    e. gestire i databreach mediante l'apposita procedura definita dall'Ente;
i) fa osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti;
j) garantisce l'evasione delle richieste degli interessati, mediante l'apposita procedura definita dall'Azienda;
k) garantisce l'evasione delle istanze del Garante per la protezione dei dati personali;
l) collabora all'individuazione dei soggetti terzi che trattano dati personali di cui l'Ente è Titolare, per conto dello stesso, ai fini della loro nomina in qualità di Responsabili esterni al trattamento ex art. 28 del GDPR.

Il Responsabile Interno del Trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al settore di competenza.

***Responsabile protezione dei dati (RPD/DPO)*:** L'Azienda ha nominato un DPO ai sensi degli artt. 37, 38 e 39 del GDPR. Il DPO è contattabile alla mail: dpo@sercop.it.

Il **Referente privacy**:

a) supporta operativamente il Responsabile interno del trattamento nell'esercizio delle proprie funzioni;
b) si interfaccia con il Responsabile Interno del trattamento, gli Incaricati, il Responsabile per la protezione dei dati (DPO), e gli altri soggetti interni ed esterni coinvolti a vario titolo, ai fini della gestione operativa delle procedure privacy;
c) cura l'aggiornamento dei regolamenti, della modulistica e dei registri adottati dall'Ente nell'ambito del sistema di protezione dei dati personali, su indicazione del Responsabile Interno del Trattamento e con il supporto del DPO, formulando anche proprie proposte in merito.

Incaricati al trattamento: L'Azienda, tramite il Responsabile Interno del Trattamento, provvede alla nomina dei dipendenti quali incaricati al trattamento dei dati personali, attraverso provvedimenti specifici di nomina ed autorizzazione al trattamento definiti in coerenza con l'assetto organizzativo aziendale e la collocazione organizzativa di ciascun dipendente. L'Incaricato del trattamento, nei limiti dell'autorizzazione allo stesso conferita dal Responsabile interno del trattamento, è tenuto a:

a) trattare i dati personali in modo lecito e secondo correttezza;
b) trattare i dati personali esclusivamente al fine di adempiere alle obbligazioni nascenti dall'incarico conferito e, in ogni caso, per scopi determinati, espliciti e, comunque, in termini compatibili con le finalità del trattamento per le quali i dati sono stati raccolti, nell'ambito del rapporto di lavoro in essere;
c) verificare costantemente la correttezza dei dati trattati e, ove necessario, richiedere il loro aggiornamento;
d) consegnare agli interessati, al momento della raccolta dei dati, i moduli contenenti l'informativa di cui all'art. 13 e/o 14 del GDPR e raccogliere il relativo consenso, quando necessario ai fini del rispetto del regolamento GDPR;
e) trattare i dati personali in maniera tale che essi risultino pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare o dal Responsabile del trattamento;
f) conservare i dati personali in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali gli stessi sono stati raccolti o successivamente trattati;
g) garantire, in ogni operazione di trattamento, la massima riservatezza. Nello specifico deve:
    a. astenersi dal trasferire, comunicare e/o diffondere i dati personali al di fuori dei soggetti destinatari individuati nel Registro dei trattamenti, salvo preventiva autorizzazione del Titolare del trattamento;
    b. svolgere operazioni di trattamento unicamente su dati/banche dati ai quali ha legittimo accesso, e utilizzare a tal fine gli strumenti indicati o messi a disposizione dall'Azienda;
h) in caso di allontanamento, anche temporaneo, dalla postazione di lavoro:
    a. per le postazioni informatiche quali personal computer o tablet o smartphone, verificare che non vi sia possibilità da parte di terzi (anche se suoi colleghi o comunque appartenenti all'Ente) di accedere ai dati personali per i quali era in corso una qualunque operazione di trattamento, sia essa mediante supporto cartaceo o informatico;
    b. per le postazioni fisiche, deve assicurare sistematicamente che, in caso di allontanamento dal posto di lavoro, i contenitori degli archivi (scrivanie, cassetti, armadi, ecc.) siano chiusi a chiave, o comunque protetti, e che i dati dagli stessi estratti non possano divenire oggetto di trattamento improprio.
i) Garantire l'aggiornamento trimestrale della/le propria/e credenziale/i di autenticazione, necessaria/e per il trattamento dei dati personali con strumenti elettronici (termine esteso a 6 mesi per le utenze amministrative), custodirle in modo sicuro ed astenersi dal comunicarle a terzi (anche se suoi colleghi o comunque appartenenti all'Azienda) in qualsiasi forma.
j) Assicura il rispetto delle misure di sicurezza riportate nel documento "*Regole generali per il trattamento dei dati personali e particolari*", consegnato in occasione dell'attribuzione della nomina a Incaricato del trattamento.

Amministratore di sistema: Devono essere nominati Amministratori di Sistema tutti coloro che, nell'espletamento delle loro consuete attività tecniche, sono "responsabili" di fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati, quali:
a) gestione dei sistemi di autenticazione e di autorizzazione;
b) custodia delle credenziali di autenticazione e di autorizzazione;
c) salvataggio dei dati (backup/recovery);
d) organizzazione dei flussi di rete;
e) gestione dei supporti di memorizzazione;

f) manutenzione e aggiornamenti hardware e software.

Possono dunque qualificarsi quali Amministratori di sistema i seguenti soggetti:
a) amministratori di sistemi di autenticazione e di autorizzazione;
b) amministratori di server e pc;
c) amministratori di apparati di rete;
d) amministratori di base di dati;
e) amministratori di apparati di sicurezza;
f) amministratori di applicazioni.

Nel caso di servizi di amministrazione di sistema affidati ad un soggetto esterno, quale Responsabile esterno del Trattamento, l'Azienda dovrà impegnarsi a conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

Qualora l'attività degli amministratori di sistema riguardi servizi o sistemi che trattano informazioni di carattere personale di dipendenti, l'Azienda è tenuta a rendere nota o conoscibile l'identità degli Amministratori di sistema nell'ambito della propria organizzazione.

4.3 Elenco dei trattamenti dei dati personali

L'elenco dei trattamenti è riportato nel Registro delle attività di trattamento ex art. 30 GDPR, del quale il presente documento costituisce parte integrante.

Il registro dei trattamenti è verificato periodicamente dal DPO ed è soggetto ad aggiornamento periodico, ogniqualvolta l'Azienda attivi nuovi trattamenti, oppure modifichi finalità e mezzi dei trattamenti in essere.

5. MODALITÀ OPERATIVE

5.1 Strutture dove sono svolti i trattamenti.

I trattamenti correnti vengono svolti presso la sede legale dell'Azienda, in Via Cornaggia, 33 a Rho (MI), nelle ulteriori sedi Ser.co.p. e comunali dove operano dipendenti dell'azienda e nelle eventuali sedi operative nelle quali vengono instaurati rapporti periodici in relazione agli specifici progetti.

5.2 Soggetti autorizzati al trattamento dei dati

Il trattamento è svolto esclusivamente dai soggetti incaricati tramite lettera di incarico scritta specificante per ogni funzione l'ambito dei trattamenti consentiti ed analitiche istruzioni scritte sulle mansioni affidate e sugli adempimenti da rispettare. Gli incaricati hanno, oltre ad applicare le regole esplicitate, il compito di informare il titolare nella eventualità che si siano rilevati dei rischi, non compresi nell'analisi dei rischi effettuata e non coperti in maniera adeguata dalle misure di sicurezza adottate.

L'elenco dei soggetti autorizzati al trattamento dei dati personali viene aggiornato annualmente in occasione della predisposizione del Piano programma aziendale.

5.3 Analisi dei rischi incombenti sui dati

Con riferimento alla struttura, i rischi possono consistere in:

- ingressi di estranei a locali/aree,
- sottrazione di strumenti contenenti dati,
- eventi distruttivi naturali (es. incendi, allagamenti, condizioni ambientali, etc.), o artificiali (es. guasto di sistemi complementari),
- errori umani nella gestione della sicurezza fisica.

Al fine di mitigare tali rischi, i locali di archiviazione dei dati sensibili e personali sono ben definiti, ed è sempre garantita la presenza di dipendenti e/o amministratori. L'accesso di estranei è controllato costantemente.

Sono inoltre attive le misure di prevenzione e protezione previste dalla legislazione vigente relative agli impianti elettrico e termico.

Con riferimento agli strumenti elettronici, i rischi possono consistere nell'azione di virus informatici o di programmi suscettibili di recare danno, nel malfunzionamento, indisponibilità o degrado degli strumenti, negli accessi esterni non autorizzati, nell'intercettazione di informazioni in rete, nella cancellazione di dati.

Il rischio di deterioramento e perdita dei dati può essere ritenuto basso grazie alla conservazione di copie di sicurezza/supporti di memorizzazione.

Con riferimento ai soggetti che trattano i dati, i rischi possono consistere nella carenza di consapevolezza, nella disattenzione o incuria, in errori materiali, o nella carente informazione.

Per far fronte a tali rischi, l'Azienda adotta specifiche misure di sicurezza informatica, ed in particolare garantisce la progressiva implementazione delle misure di sicurezza previste dalla Circolare Agid n. 2/2017, a partire dalle misure di sicurezza minime. Con frequenza annuale, le misure di sicurezza AGID sono verificate mediante appositi audit dal DPO, attestate dal Responsabile Interno del Trattamento e registrate nel modulo di implementazione di cui all'Allegato 2 della suddetta Circolare.

L'analisi dei rischi e la verifica delle misure di sicurezza organizzative, analogiche ed informatiche implementate viene effettuata con frequenza annuale, attraverso l'utilizzo della "*Check list compliance privacy-GDPR - Valutazione dei rischi e posizionamento dell'ente*". Tale checklist viene verificata dal DPO, con il supporto del Responsabile Interno del Trattamento, del Referente privacy, degli Amministratori di sistema e delle altre figure aziendali che si ritiene di coinvolgere. La check list verifica il posizionamento dell'Azienda, ne valuta l'esposizione ai rischi, individua le azioni di mitigazione dei rischi e le tempistiche di attuazione con riferimento ai seguenti aspetti:

- contesto;
- organizzazione;
- misure informatiche;
- misure analogiche;
- compliance GDPR;
- compliance AGID;
- posizionamento complessivo.

5.4 Modalità dei trattamenti

5.4.1 Informativa privacy agli interessati

Ad ogni interessato viene rilasciata, nei tempi e nei modi previsti dagli artt. 13 e 14 del GDPR, un'informativa relativa ai dati personali trattati. L'informativa viene sempre sottoscritta dall'interessato per presa visione.

La modulistica relativa viene conservata unitamente agli atti connessi alla pratica in ragione della quale si è rilevato l'obbligo di presentare l'informativa in modo da garantire la possibilità di dimostrare l'avvenuto rilascio dell'informativa

Durante lo svolgimento delle attività possono inoltre essere richieste specifiche autorizzazioni relative al trattamento di particolari dati personali, qualora non coperti dall'informativa iniziale.

Il trattamento può avvenire sia mediante archivi e strumenti informatici, sia attraverso archivi fisici e cartacei.

5.4.2 Misure generali di sicurezza

Sono state approntate alcune misure generali, per fronteggiare soprattutto i rischi derivanti da carenza di informazioni e di controllo. In particolare:

- Sono stati specificati nelle lettere di incarico i compiti e gli accorgimenti necessari da seguire nel corso delle attività lavorative;
- Per i trattamenti in qualità di responsabile, la specificazione degli ambiti di trattamento consentiti e dei compiti assegnati è effettuata sulla base di quanto specificato dal titolare del trattamento svolto;
- Sono previsti opportuni approfondimenti periodici in tema di sicurezza nel corso delle riunioni di staff e lo svolgimento di corsi periodici annuali.
- È stata data istruzione ai responsabili dei singoli servizi affinché avvisino il Responsabile Interno del Trattamento di ogni fattispecie che comporti, in capo a personale dipendente o incaricato da Ser.co.p., la variazione nel perimetro dei dati personali di cui è possibile il trattamento;
- E' stata data istruzione, a tutti i dipendenti e collaboratori, circa l'obbligo di segnalazione di ogni anomalia riscontrata.

Particolare attenzione viene posta alla definizione di procedure che garantiscano la tutela dei dati da parte degli operatori del protocollo. Nella fase di acquisizione di atti e documenti, gli incaricati del protocollo, dopo aver adempiuto ai compiti d'ufficio, devono garantire che i dati e le informazioni, digitali e non, siano trasmesse direttamente agli incaricati di riferimento.

5.4.3 Misure di sicurezza per i trattamenti non elettronici

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

- Si dispone che gli incaricati non lascino incustoditi sulle scrivanie, o su altri ripiani o in luoghi facilmente accessibili a personale non autorizzato atti, documenti e fascicoli contenenti dati personali, ma li conservino in appositi schedari/fascicoli, prelevandoli solo per il tempo necessario al trattamento.
- Gli armadi destinati all'archivio di dati personali relativi agli utenti dei singoli servizi sono chiusi a chiave. Tutti gli incaricati al trattamento hanno inoltre funzioni di controllo dell'accesso agli archivi, situati in locali con possibilità di chiusura a chiave in caso di non presenza di personale autorizzato al trattamento.

- Nel caso in cui incaricati al trattamento Ser.co.p. debbano, per esclusive ragioni di servizio, accedere a dati o informazioni sui quali non abbiano specifica autorizzazione al trattamento ne informano preventivamente il proprio responsabile organizzativo che si raccorda con il responsabile dell'ufficio avente titolo al fine di concordate tempi e modi di accesso ai dati oggetto di richiesta.
- Il personale dipendente e i collaboratori a qualsiasi titolo sono comunque sensibilizzati al controllo circa la costante chiusura a chiave di tali archivi e relativamente alla presenza del personale nei locali contenenti tali archivi: qualsiasi anomalia deve essere immediatamente segnalata al Responsabile Interno del Trattamento dei dati.
- E assolutamente vietato utilizzare come "carta da riciclo": documenti contenenti dati personali, soprattutto per stampa di altri documenti: tali documenti devono essere distrutti, mediante l'apposito "trituratore".

5.4.4 Misure di sicurezza per il trattamento con strumenti elettronici

Regole generali per gli incaricati al trattamento dei dati personali

Nell'informativa consegnata agli incaricati ai sensi del precedente punto 5.2 sono previste specifiche istruzioni per l'utilizzo della posta elettronica e di Internet, circoscrivendone l'utilizzo alle necessità lavorative sulla base della discrezione e del senso di responsabilità di ogni operatore. Tali istruzioni sono contenute nel documento "REGOLE GENERALI PER IL TRATTAMENTO DEI DATI PERSONALI", allegato al presente documento e consegnato a ciascun dipendente/collaboratore incaricato del trattamento. Nei successivi paragrafi si riprendono tali norme:

- Nella fase di gestione, tutti i dati e le informazioni personali sono trattati dagli operatori incaricati sotto la loro diretta responsabilità e vigilanza.
- Gli incaricati assicurano che soggetti non autorizzati accedano, anche incidentalmente, alle informazioni di cui sono autorizzati al trattamento e delle quali si trovino in possesso. Al fine di prevenire eventuali rischi di accesso indebito gli incaricati, in caso di assenza temporanea dal PC, procedono ad attivare il blocco dello schermo o altre modalità che impediscano l'accesso a PC da parte di soggetti non autorizzati.
- La modifica dei componenti interni (aggiunta, rimozione, sostituzione) delle attrezzature informatiche messe a disposizione dall'Azienda, nonché la modifica delle configurazioni software impostate sulla propria o altrui postazione di lavoro è consentita esclusivamente ai soggetti appositamente incaricati dall'Ente.
- Nell'utilizzo delle risorse informatiche personali (tablet, smartphone, notebook, ecc.) , che deve essere sempre comunicato e autorizzato in forma scritta dal Dirigente di riferimento, l'incaricato garantisce il rispetto delle medesime cautele previste nell'ambito dell'utilizzo dei dispositivi aziendali, garantendo l'aggiornamento costante dei software e la presenza di un efficace antivirus. L'Amministratore di sistema tiene traccia in un apposito registro delle risorse informatiche private autorizzate all'uso presso l'Azienda. In caso di autorizzazione all'uso di risorse informatiche private, il dipendente autorizzato è tenuto a rispettare le configurazioni di sistema dell'Azienda e a garantire il rispetto delle misure minime di sicurezza descritte nella circolare AGID n. 2/2017.
- Nelle sedi aziendali non è consentito l'utilizzo di dispositivi di connessione web personali. Nel caso di prestazioni rese in lavoro agile è consentito connettere la strumentazione aziendale a dispositivi di connessione web personali (es. modem, tethering, bluetooth, …)

a condizione che nell'utilizzo di detti dispositivi:
    - si attivi esclusivamente la connessione VPN aziendale;
    - si garantisca che i dati personali sui dispositivi aziendali non possano essere accessibili a terze parti connesse al medesimo dispositivo di connessione;
    - che siano attivati (in caso di tethering) strumenti di protezione del dispositivo personale da virus e sw/codici maligni.
- In caso di smarrimento o furto di dispositivi informatici, oltre a sporgere regolare denuncia all'autorità competente, occorre effettuare tempestivamente la segnalazione di databreach al Referente privacy, utilizzando il modulo previsto nell'apposita procedura.
- Per quanto riguarda l'utilizzo di dispositivi mobili (notebook, tablet, smartphone, ecc.), sono richieste ulteriori precauzioni, rispetto alle postazioni fisse, con particolare riferimento a:
    - attenzione rispetto al furto o allo smarrimento;
    - attenzione rispetto a virus o codici maligni tramite reti wireless.
- I dispositivi mobili che rimangono sconnessi a lungo dalla rete non ricevono gli aggiornamenti automatici e possono avere quindi un livello di protezione non allineato con gli standard dell'Azienda. È quindi a carico dell'utilizzatore garantire la funzionalità e l'aggiornamento del sistema.
- Per quanto riguarda le smart card, business key e altri dispositivi per il riconoscimento che contengono certificati di firma dei titolari, utilizzabili ad esempio nei procedimenti amministrativi dell'Azienda, i destinatari sono responsabili del corretto utilizzo e devono custodire adeguatamente i dispositivi, il relativo PIN e altro materiale a corredo. Essi, inoltre, garantiscono il costante aggiornamento dei dispositivi, secondo le indicazioni fornite dal produttore.
- Non è consentito navigare in internet in siti non attinenti allo svolgimento delle mansioni assegnate. Non è consentito trasferire sulla propria postazione di lavoro, neanche temporaneamente, mediante download, file o programmi da siti sconosciuti che potrebbero compromettere il funzionamento del computer, o comunque materiale non pertinente all'attività lavorativa.
- Non è consentito l'uso di programmi peer-to-peer per lo scambio di file in ambito privato.
- Non è consentito partecipare, a meno di esigenze professionali, a siti di chat, forum e/o social network.

Accesso a mail e sistemi informatici

Per ridurre i rischi relativi agli strumenti elettronici sono state adottate le seguenti misure di sicurezza:

- Sono stati implementati profili autorizzativi che consentono ad ogni incaricato l'accesso ai soli dati per i quali è stato autorizzato al trattamento.
- Ciascun incaricato viene dotato di un proprio username e di una password di minimo 8 (otto) caratteri, che va cambiata al primo accesso. La password non contiene elementi facilmente ricollegabili all'Azienda o all'incaricato. Ogni tre mesi ciascun incaricato è tenuto a sostituire la propria password. Per le password di dominio tale misura diviene operativa entro il 1° trimestre 2023.
- Al fine di tutelare eventuali dati personali del lavoratore, Ser.co.p. favorisce l'utilizzo di caselle di posta elettronica nominative (secondo lo schema nome.cognome@sercop.it), garantendo l'esclusivo accesso da parte del titolare della mail. Nel corso del 2023 Ser.co.p.

si adopererà per limitare la creazione di account condivisi (es. nomeufficio@sercop.it), attivando, qualora si renda necessaria l'attivazione di simili account, strumenti per la "personalizzazione" della gestione al fine di permettere al destinatario delle e-mail di risalire con certezza al mittente delle mail (es. alias).

- Gli utenti del sistema informatico sono qualificati con profili di power user o user che limitano l'azione sul sistema del PC.
- Il sistema è configurato affinché, se l'operatore non agisce per più di 10 minuti, lo schermo viene bloccato richiedendo la password per poter riaccedere. In fase di installazione viene verificato il blocco automatico della singola postazione. Con l'attivazione delle nuove policy di dominio, entro il 1° trimestre 2023, la misura sarà operativa a livello centralizzato.
- È in fase di elaborazione un manuale interno di corretto uso dei sistemi informatici, nel quale verrà disciplinato il biocco automatico di cui al punto precedente.
- Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
- In caso di perdita della qualità di incaricato al trattamento dei dati personali in possesso di Ser.co.p. procede alla disattivazione delle password secondo la seguente procedura:
  - Alla cessazione dello status di incaricato al trattamento il servizio Risorse Umane comunica la cessazione all'Amministratore di sistema che procede tempestivamente alla modifica della password di accesso a e-mail, banche dati e ad altri sistemi al fine di inibire l'accesso a soggetti non più titolati a ciò;
  - L'Amministratore di sistema attiva, sulle caselle e-mail su cui agiva, in nome di Ser.co.p., il soggetto non più Incaricato del trattamento, un sistema di risposta automatica nel quale si indica il recapito mail sostitutivo cui il mittente può inoltrare le mail in sostituzione dell'indirizzo in via di disattivazione. Viene inibito l'invio di comunicazioni dall'indirizzo e-mail in via di disattivazione;
  - Trascorsi 60 giorni, l'Amministratore di sistema procede alla cancellazione dei messaggi contenuti nella casella e-mail e alla disattivazione della medesima casella.
  - Nel medesimo termine si procede alla disattivazione di tutte le password.

Aggiornamento software in uso dall'incaricato

Sono state realizzate misure di protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici: in particolare ogni computer è dotato di antivirus, aggiornato periodicamente con inibizione della possibilità di blocco degli aggiornamenti. In particolare:

- L'aggiornamento dei Sistemi Operativi è gestito in modo automatico, secondo i tempi di rilascio delle software house.
- L'aggiornamento dei software di produttività (es. Office, ecc.) è gestito in modo centralizzato e automatico, secondo i tempi di rilascio delle software house.
- È stato disposto l'obbligo di provvedere alla memorizzazione delle banche dati e dei dati personali contenuti nel server (copie di back-up); tale attività viene svolta giornalmente in maniera automatica dal server.

Utilizzo di dispositivi rimovibili

Al fine di garantire la protezione dei dati e alla minimizzazione degli impatti negativi in caso di eventi

fortuiti è possibile utilizzare, in connessione alla strumentazione aziendale, solo dispositivi rimovibili (es. chiavette USB, SD card, hard disk esterni, ecc.) forniti dall'Azienda. A tal fine gli Incaricati, in caso di esigenze particolari e motivate, possono fare richiesta all'Azienda di dispositivi rimovibili per l'utilizzo temporaneo di dati posti sotto la titolarità Ser.co.p. L'incaricato deve utilizzare i supporti rimovibili Ser.co.p. secondo i criteri generali di diligenza, al pari dell'altra strumentazione in dotazione Ser.co.p. In nessun caso è possibile utilizzare i dispositivi rimovibili, quali strumento di back up unico dei dati utilizzati in quanto tale funzione è ottemperata dai server Ser.co.p. che automaticamente effettuano quotidianamente il backup dei dati.
L'utilizzo dei dispositivi rimovibili, pertanto, deve considerarsi di natura eccezionale per la temporanea conservazione di dati per esigenze particolari e/o per il trasferimento di dati da un dispositivo ad un altro, quando non siano utilizzabili altre modalità.
Con riferimento all'utilizzo dei supporti rimovibili si richiamano le seguenti regole aziendali:

- L'incaricato, a qualsiasi titolo, del trattamento garantisce che sui dispositivi rimovibili siano conservati esclusivamente i dati necessari strettamente necessari all'utilizzo in uno specifico e circoscritto contesto al di fuori degli ambienti lavorativi, ma con finalità esclusivamente connesse all'attività svolta presso Ser.co.p. E' fatto divieto di utilizzare i dispositivi rimovibili quale strumento di backup, stante la presenza di backup automatici dei server Ser.co.p.
- E' fortemente sconsigliato l'utilizzo di supporti rimovibili per il salvataggio e la conservazione di dati personali e, in ogni caso, è vietato l'utilizzo di supporti rimovibili ad utilizzo "promiscuo" personale/aziendale. E' proibito duplicare documenti contenenti dati particolari su supporti rimovibili o su sistemi di rete non gestiti dal personale dell'Ente.
- Qualora vengano utilizzati supporti rimovibili di proprietà dell'Azienda, l'utilizzatore adotta ogni precauzione a che tali supporti vengano utilizzati esclusivamente per il trattamento di dati inerenti al Suo perimetro di autorizzazione evitando sia l'utilizzo di detti dispositivi per la conservazione di dati extra-lavorativi, sia l'utilizzo dei supporti rimovibili su apparecchiature di dubbia o di nulla protezione/aggiornamento della protezione con antivirus. Nel caso non conoscenza del sistema di protezione in uso sulla specifica apparecchiatura, l'incaricato deve, prudenzialmente, considerarla come "non protetta" e quindi non utilizzare su di essa supporti rimovibili aziendali.
- E' sempre raccomandata la massima cura dei supporti rimovibili in dotazione agli incaricati del trattamento dei dati, in particolare l'incaricato dovrà garantire costantemente che nessuno possa accedere, prendere visione o trarre copia, anche incidentalmente, dei dati contenuti nei supporti rimovibili in proprio possesso.
- Al termine del rapporto di lavoro/collaborazione ovvero in caso di variazione del ruolo aziendale l'incaricato del trattamento riconsegna all'Azienda i supporti rimovibili in uso, con l'assoluto divieto di effettuare copie dei contenuti. L'Amministratore di sistema prende in carico i dispositivi riconsegnati e, dopo averne fatto copia sui server aziendali, stabilisce se procedere alla formattazione dei medesimi ovvero, qualora si rilevi anche in potenza il rischio di recupero dei dati precedentemente salvati, alla distruzione. Nel caso in cui non sia possibile, al di sopra di ogni ragionevole dubbio, il recupero dei dati contenuti nei supporti l'Amministratore di sistema rimette nella disponibilità dell'Azienda il supporto rimovibile.
- Si considerano sempre autorizzati i dispositivi mobili abilitati per la firma digitale e quelli esplicitamente autorizzati dal Responsabile del trattamento.

L'Amministratore di sistema tiene traccia in un apposito registro dei dispositivi rimovibili in uso e/o autorizzati presso l'Azienda.

Utilizzo di cloud esterni

L'azienda definisce la possibilità di utilizzo di sistemi cloud (es. google drive, dropbox, ecc.), per la gestione di progetti e attività con altri partner, che comportino il trattamento di dati personali, individuando il (o i) sistemi esplicitamente autorizzati. E' da intendersi vietato l'utilizzo di sistemi cloud non esplicitamente autorizzati dall'Azienda.

Accesso a mail e sistemi informatici in caso di assenza dell'incaricato

Il Titolare del trattamento, in caso di esigenze urgenti e indifferibili, assicura la disponibilità di dati e delle informazioni contenute in cartelle personali degli incaricati che risultino assenti dal servizio. L'urgenza e l'indifferibilità è definita caso per caso in ragione delle esigenze che portano alla richiesta di disponibilità dei dati e dalla tempestività con cui i dati devono essere messi a disposizione e in ragione della presenza di ragioni di sicurezza o di esigenza di garantire l'ordinaria operatività.
La richiesta di dati deve avvenire in forma scritta da parte dell'Interessato richiedente che ne fa domanda al proprio responsabile organizzativo, indirizzando tale richiesta per conoscenza al responsabile organizzativo dell'incaricato in possesso dei dati richiesti, l'incaricato medesimo, l'Amministratore di sistema e il referente per la privacy. La richiesta non può essere generica ma specifica e circostanziata.
Il responsabile organizzativo dell'incaricato in possesso delle informazioni, di concerto con il Dirigente di riferimento del richiedente e il referente privacy, valutano la sussistenza delle condizioni di urgenza e indifferibilità e l'impossibilità oggettiva di attendere il rientro dell'interessato in possesso dei dati per la soluzione della specifica fattispecie.
A fronte dell'esito positivo della richiesta, l'Amministratore di sistema mette a disposizione dell'incaricato richiedente i dati, le cartelle e le informazioni richieste, procedendo al reset della password dell'interessato assente, che al rientro provvederà a definire una nuova password di accesso alle cartelle o alla caselle e-mail.
L'accesso sarà comunque limitato ai soli documenti necessari per fini lavorativi.

5.4.5 Misure e procedure aziendali: implementazione e aggiornamento

L'Azienda garantisce la progressiva implementazione delle misure di sicurezza previste dalla Circolare dalla Circolare Agid n. 2/2017, a partire dalle misure di sicurezza minime. Con frequenza annuale, le misure di sicurezza AGID sono verificate mediante appositi audit dal DPO, attestate dal Responsabile Interno del Trattamento e registrate nel modulo di implementazione di cui all'Allegato 2 della suddetta Circolare.
In ragione del continuo evolversi delle minacce, vanno considerate parte integrante delle presenti misure, ogni comunicazione o istruzione che l'Azienda riterrà opportuno inviare agli incaricati del trattamento in ragione di eventi di sicurezza specifici, dell'introduzione di nuove tecnologie e degli avvisi rilasciati dal CSIRT Italia o dal CERT Agid.
Sarà inoltre adottata ogni altra misura che venisse ritenuta utile e necessaria dai tecnici, compatibilmente alle risorse disponibili, per migliorare la sicurezza degli strumenti elettronici.

5.4.6 Misure per il ripristino dei dati

I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici (anti virus,

anti Worm, protezione da programmi maligni in genere) che verranno aggiornati automaticamente o da persone a tal fine incaricate, con cadenza periodica, anche giornaliera.

Si provvede inoltre, periodicamente e secondo le criticità rilevate, tramite persone a tal fine incaricate, all'aggiornamento dei programmi per l'elaborazione volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne i difetti.

Giornalmente viene effettuato il back up automatico, su NAS, su supporto rimovibile e in cloud, di tutti i dati contenuti nei server dell'amministrazione.

In caso di danneggiamento degli archivi contenenti dati particolari o giudiziari o degli strumenti elettronici, sono attive idonee misure per garantire il ripristino dell'accesso ai dati in tempi certi compatibili con i diritti degli interessati, potendo ripristinare la situazione al giorno precedente in un tempo di circa 6 ore.

Nell'ipotesi di distruzione o danneggiamento dei dati particolari e/o dati relativi a condanne penali e reati, o degli strumenti elettronici che li contengono, si adotterà la seguente procedura:

- L'amministratore di sistema chiederà immediatamente l'intervento della ditta addetta alla manutenzione sollecitandone al più presto l'assistenza;
- il tecnico 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 back-up e provvedendo al loro aggiornamento;
- verrà richiesto al tecnico della manutenzione di suggerire ogni altra misura necessaria e di verificare comunque l'efficacia della sostituzione, oltre a rilasciare certificazione scritta circa l'intervento effettuato.

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

5.4.7 Formazione continua degli incaricati

La formazione degli incaricati viene effettuata all'atto della nomina e dell'assunzione dei compiti relativi, in caso di variazioni significative nelle mansioni assegnati, che comportino un cambiamento significativo delle modalità di trattamento dei dati personali, e ogni qualvolta se ne presenti la necessità, a fronte di modifiche e aggiornamenti delle misure di sicurezza, delle pratiche operative, di situazioni che richiedano particolari accorgimenti o di modifiche legislative che impattino con le regole presenti in questo documento. 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 particolari.

La formazione è svolta a cura di personale competente in materia.

Il titolare verifica comunque perlomeno annualmente, sulla base delle verifiche svolte e, delle eventuali problematiche riscontrate, la necessità di provvedere a formazione specifica.

La formazione effettuata viene registrata su apposita modulistica e viene verificata dal DPO.

5.4.8 Procedura di dismissione sicura dei dispositivi elettronici, dei pc e dei device aziendali

Qualora si decida di procedere alla dismissione e allo smaltimento di uno o più dispositivi elettronici, pc o device aziendali non utilizzati, il Responsabile interno del trattamento (Direttore) trasmette

una comunicazione scritta all'Amministratore di sistema, richiedendo di procedere alla dismissione ed allo smaltimento e specificando i dispositivi da dismettere, mediante gli estremi identificativi dell'inventario.

L'Amministratore di sistema procede al ritiro dei dispositivi, attivandosi per la cancellazione sicura e certificata dei dati personali in essi contenuti e lo smaltimento di rifiuti elettrici ed elettronici, anche mediante il ricorso a soggetti specializzati, nel rispetto delle indicazioni fornite dal Garante privacy (Provv. del 13/10/2008) e delle migliori prassi vigenti in materia.

In particolare, la cancellazione sicura e certificata può avvenire mediante metodi quali:

a) procedure di data wiping o file shredding, tramite l'utilizzo di software dedicati, che ne certifichino anche il processo;
b) de-magnetizzazione del disco tramite degaussing elettromagnetico, procedimento che utilizza un accumulo di energia elettrica e quando questo raggiunge il livello necessario, una scarica genera un campo magnetico in grado di rimuovere i dati in modo sicuro e definitivo da ogni superficie magnetica, rendendo il dispositivo totalmente inutilizzabile;
c) distruzione fisica del disco, preferibilmente effettuata presso centri specializzati o presso la sede dell'Amministratore di sistema. Dev'essere fornita una specifica documentazione che tracci tutto il procedimento di distruzione, certificandone la conformità a norma.

L'Amministratore di sistema sottopone al Responsabile interno del trattamento un preventivo di spesa per la dismissione e lo smaltimento presentando, se opportuno, più alternative possibili.

Il Responsabile interno del trattamento procede con l'autorizzazione della spesa, individuando, quando previsto, la procedura da seguire tra quelle proposte dall'Amministratore di sistema.

L'Amministratore di sistema procede alla dismissione e allo smaltimento dei dispositivi, secondo le modalità individuate.

Al termine della procedura di dismissione e di smaltimento, l'Amministratore di sistema trasmette al Responsabile interno del trattamento un report comprendente tutte le certificazioni acquisite in merito alle procedure di cancellazione sicura, dismissione e smaltimento adottate.

5.4.9 Trattamento da parte di soggetti esterni

Il trattamento di dati personali da parte di soggetti esterni che operano per conto di SER.CO.P. è regolamentato all'interno dei capitolati di appalto, dei contratti che regolano la fornitura dei servizi affidati, oppure mediante accordi integrativi degli stessi. Tali soggetti sono nominati Responsabili del trattamento, e mediante gli atti pocanzi citati sono definiti ruoli, responsabilità e limiti dei trattamenti loro affidati, nonché sono impartite apposite istruzioni documentate sul trattamento, secondo i termini e le modalità di cui all'art. 28 del GDPR.

ALLEGATO A: REGOLE GENERALI PER IL TRATTAMENTO DEI DATI PERSONALI

REGOLE PER IL TRATTAMENTO DI DATI PERSONALI E PARTICOLARI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Nel trattamento dei dati personali e particolari Le chiediamo di osservare le seguenti istruzioni finalizzate al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento, da parte Sua, durante le operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

Nella fase di acquisizione di atti e documenti, l'incaricato del protocollo, dopo aver adempiuto ai compiti d'ufficio, deve garantire che i supporti cartacei contenenti i dati e le informazioni vengano trasmessi direttamente ai responsabili di riferimento senza conservazione presso gli uffici dedicati al protocollo.

Gli atti, i documenti e i fascicoli contenenti dati personali, particolari o giudiziari che Le saranno affidati per lo svolgimento dei relativi compiti dovranno essere conservati in appositi schedari/fascicoli e da Lei controllati e custoditi per le attività necessarie garantendo che ad essi non accedano persone prive di autorizzazione. Nel caso in cui i documenti debbano essere restituiti ad un incaricato, il possesso dei documenti, degli atti e dei fascicoli deve avvenire per il tempo necessario per lo svolgimento delle pratiche di competenza del Suo ufficio e, al termine delle operazioni affidate, dovranno essere da Lei restituiti. In occasione di ricevimento pubblico, occorre evitare di lasciare sulla scrivania documentazione cartacea contenente dati personali di altri soggetti.

E assolutamente vietato riciclare documenti contenenti dati personali, soprattutto per stampa di altri documenti: tali documenti devono essere distrutti, mediante l'apposito "trituratore".

Tutta la documentazione cartacea è archiviata in appositi armadi dotati di serratura. I singoli atti e documenti amministrativi devono essere archiviati. In assenza di operatori di riferimento all'interno degli uffici, gli armadi devono essere chiusi a chiave e la chiave conservata in un posto sicuro.

L'accesso ad archivi non di Sua pertinenza, per esclusive esigenze di servizio, è sempre oggetto di richiesta motivata al Suo responsabile organizzativo, cui il medesimo, di concerto con l'incaricato al trattamento dei dati richiesti, darà risposta scritta di autorizzazione o di diniego. La procedura di richiesta è definita nel Regolamento sulle misure di sicurezza per il trattamento dei dati personali ex art. 32 Reg. UE 679/2016 (GDPR) Ser.co.p., approvato con Del. xx del CdA del XX/12/2022.

REGOLE PER IL TRATTAMENTO DI DATI PERSONALI E PARTICOLARI CON L'AUSILIO DI STRUMENTI ELETTRONICI

Le persone autorizzate all'accesso ai dati personali con strumenti elettronici verranno dotate di apposita credenziale di autenticazione che consente il superamento di una procedura di autenticazione e autorizzazione relativa al trattamento al quale Lei è stato abilitato.

Utilizzo delle credenziali di autenticazione

La credenziale di autenticazione consegnata consiste in un codice per la Sua identificazione (**USER ID**) associato a una parola chiave (**PASSWORD**) riservata e conosciuta solamente da Lei. Lei deve custodire le credenziali di autorizzazione in modo sicuro ed astenersi dal comunicarle a terzi (anche se Suoi colleghi o comunque appartenenti alla struttura) in qualsiasi forma.

La parola chiave è composta, e ogniqualvolta Lei la modificherà dovrà essere composta, da almeno otto caratteri alfanumerici maiuscoli e minuscoli intervallati da caratteri speciali e non dovrà contenere riferimenti agevolmente a Lei riconducibili. Le norme di sicurezza in materia di protezione dei dati dispongono che la prima password deve essere modificata dall'Incaricato al Trattamento dei dati al primo utilizzo e, successivamente, almeno ogni tre mesi.

Le precisiamo che, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica, le credenziali di autenticazione saranno disattivate nei casi di non utilizzo da almeno sei mesi e di eventuale perdita della qualità di incaricato al trattamento che Le consenta l'accesso ai dati personali.

La informiamo che in caso di assenza o impossibilità, temporanea o protratta nel tempo, di un dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata e in uscita, il dirigente di riferimento del dipendente effettua una comunicazione scritta all'Amministratore di sistema, inoltrandola per conoscenza al Direttore generale, per richiedere l'accesso alla postazione e/o alla casella di posta elettronica del dipendente assente. Contestualmente, il dirigente di riferimento del dipendente deve informare il dipendente appena possibile, fornendo adeguata motivazione.

Utilizzo della propria postazione di lavoro

Ogni operatore può accedere ad una postazione di lavoro dotata anche di hardware e software indispensabili per il trattamento digitalizzato dei dati, mediante l'utilizzo di proprie credenziali di accesso. Le richiediamo di utilizzare la postazione di lavoro con l'ordinaria diligenza, evitando di scaricare ed installare sul P.C. assegnato, software non autorizzati. In ogni caso, il download e l'aggiornamento di software viene inibito agli utenti con profilo user e viene gestito direttamente dall'Amministratore di sistema. La richiesta di installazione e/o aggiornamento di un software deve essere inoltrata all'Amministratore di sistema via mail.

Le postazioni devono essere utilizzate esclusivamente per attività inerenti all'attività lavorativa per l'Azienda. Le informazioni e i dati trattati devono essere archiviati sulle risorse locali, di rete o in cloud indicate dall'Azienda.

Non è consentito lasciare una postazione incustodita accesa o non bloccata, soprattutto se connessa alla rete. Qualora ci si allontani, anche temporaneamente, dalla propria postazione, occorre bloccare il computer (attivare la schermata di protezione) o disconnettersi.

Misure di sicurezza e protezione dei dati personali

La informiamo che i dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale, mediante l'attivazione di idonei strumenti elettronici (anti virus, firewall, protezione da programmi maligni in genere) che verranno aggiornati automaticamente o da persone a tal fine incaricate, con cadenza periodica anche giornaliera. Dovrà pertanto seguire le particolari regole di sicurezza e nel caso di virus dovrà chiamare l'Amministratore di sistema che curerà detto intervento.

Si provvederà inoltre, periodicamente e secondo le criticità rilevate, tramite persone a tal fine incaricate, all'aggiornamento dei programmi per l'elaborazione volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne i difetti.

Giornalmente viene effettuato il back up automatico, sia su dispositivi in locale, sia in cloud, di tutti i dati contenuti nei server dell'amministrazione: è quindi suo compito salvare tutti i file informatici da Lei creati o modificati, con le modalità definite e nel rispetto dell'architettura del sistema precostituita.

La informiamo che, per il caso di danneggiamento degli archivi contenenti dati particolari o giudiziari o degli strumenti elettronici, abbiamo adottato idonee misure per garantire il ripristino dell'accesso ai dati in tempi certi compatibili con i diritti degli interessati, potendo ripristinare la situazione al giorno precedente in un tempo di circa 6 ore.

Utilizzo della casella mail aziendale

Lei è tenuto a utilizzare la casella di posta elettronica d'ufficio esclusivamente per ragioni di servizio, e a verificare che sia disattivata l'anteprima automatica dei file nei client di posta utilizzati. È comunque necessario porre particolare attenzione ad aprire allegati compressi o contenenti programmi "eseguibili" ed effettuare sempre un controllo antivirus preventivo. È fatto divieto di usare per scopi istituzionali caselle di posta elettronica di provider diversi da quello istituzionale (es. libero, gmail, ecc.).

Utilizzo di dispositivi informatici

Non è consentito utilizzare dispositivi rimovibili come chiavette USB o dischi portatili da collegare alle singole postazioni d'ufficio, ad eccezione dei dispositivi abilitati per la firma digitale e degli altri dispositivi rimovibili aziendali espressamente autorizzati in forma scritta dal dirigente di riferimento. L'Amministratore di sistema tiene traccia in un apposito registro dei dispositivi rimovibili in uso presso l'Azienda.

Tali dispositivi devono essere custoditi in cassetti chiusi a chiave.

Nel caso Lei dovrà effettuare operazioni di trattamento di dati personali con copie o supporti rimovibili contenenti detti dati, si rimanda al Regolamento sulle misure di sicurezza per il trattamento dei dati personali ex art. 32 Reg. UE 679/2016 (GDPR). Si richiama il divieto di duplicare documenti contenenti dati particolari su supporti rimovibili o su sistemi di rete non gestiti dal personale dell'Ente (ad es. su cloud esterno) È vietato l'utilizzo di sistemi di cloud (es. google drive, dropbox, ecc.) non autorizzati espressamente dall'Azienda, per la gestione di progetti e attività con altri partner, che comportino il trattamento di dati personali**.**

La modifica dei componenti interni (aggiunta, rimozione, sostituzione) delle attrezzature informatiche messe a disposizione, nonché la modifica delle configurazioni software impostate sulla propria o altrui postazione di lavoro è consentita esclusivamente ai soggetti appositamente incaricati dall'Azienda.

Non è consentito utilizzare risorse informatiche private (tablet, smartphone, periferiche etc.), salvo preventiva ed esplicita autorizzazione scritta da parte del suo dirigente di riferimento. L'Amministratore di sistema tiene traccia in un apposito registro delle risorse informatiche private autorizzate all'uso presso l'Azienda. In caso di autorizzazione all'uso di risorse informatiche private, Lei è tenuto a rispettare le configurazioni di sistema dell'Azienda e a garantire il rispetto delle misure minime di sicurezza descritte nella circolare AGID n. 2/2017.

Nelle sedi aziendali non è consentito l'utilizzo di dispositivi di connessione web personali. Nel caso di prestazioni rese in lavoro agile è consentito connettere la strumentazione aziendale a dispositivi di connessione web personali (es. modem, tethering, bluetooth, …) a condizione che nell'utilizzo di detti dispositivi:

- si attivi esclusivamente la connessione VPN aziendale;
- si garantisca che i dati personali sui dispositivi aziendali non possano essere accessibili a terze parti connesse al medesimo dispositivo di connessione;
- che siano attivati (in caso di tethering) strumenti di protezione del dispositivo personale da virus e sw/codici maligni.

In caso di smarrimento o furto di dispositivi informatici, oltre a sporgere regolare denuncia all'autorità competente, occorre effettuare tempestivamente la segnalazione di databreach al Referente privacy, utilizzando il modulo previsto nell'apposita procedura.

Per quanto riguarda l'utilizzo di dispositivi mobili (notebook, tablet, smartphone, ecc.), sono richieste ulteriori precauzioni, rispetto alle postazioni fisse, con particolare riferimento a:

- attenzione rispetto al furto o allo smarrimento;
- attenzione rispetto a virus o codici maligni tramite reti wireless.

I dispositivi mobili che rimangono sconnessi a lungo dalla rete non ricevono gli aggiornamenti automatici e possono avere quindi un livello di protezione non allineato con gli standard dell'Azienda. È quindi Suo compito garantire la funzionalità e l'aggiornamento del sistema.

Per quanto riguarda le smart card, business key e altri dispositivi per il riconoscimento che contengono certificati di firma dei titolari, utilizzabili ad esempio nei procedimenti amministrativi dell'Azienda, i destinatari sono responsabili del corretto utilizzo e devono custodire adeguatamente i dispositivi, il relativo PIN e altro materiale a corredo. Essi, inoltre, garantiscono il costante aggiornamento dei dispositivi, secondo le indicazioni fornite dal produttore.

Navigazione in internet, social network e download di file

Non è consentito navigare in internet in siti non attinenti allo svolgimento delle mansioni assegnate. Non è consentito trasferire sulla propria postazione di lavoro, neanche temporaneamente, mediante download, file o programmi da siti sconosciuti che potrebbero compromettere il funzionamento del computer, o comunque materiale non pertinente all'attività lavorativa.

Non è consentito l'uso di programmi peer-to-peer per lo scambio di file in ambito privato.

Non è consentito partecipare, a meno di esigenze professionali, a siti di chat, forum e/o social network.

Disposizioni finali

Le ricordiamo che Lei è tenuto ad adottare e rispettare qualsiasi indicazione o istruzione riceverà dall'Azienda o dal Servizio Informatico, finalizzata al corretto uso degli strumenti informatici ed alla tutela della sicurezza dei dati.

In ragione del continuo evolversi delle minacce, vanno considerate parte integrante delle presenti misure, ogni comunicazione o istruzione che l'Azienda riterrà opportuno inviare agli incaricati del trattamento in ragione di eventi di sicurezza specifici, dell'introduzione di nuove tecnologie e degli avvisi rilasciati dal CSIRT Italia o dal CERT Agid.

Luogo e data, _____

Per ricevuta**, il Dipendente**

_____