REGOLAMENTO PRIVACY

PER IL TRATTAMENTO DEI DATI PERSONALI AI SENSI REG.679/2016

MISURE PER LA SICUREZZA DEL TRATTAMENTO DEI DATI PERSONALI

LINEE GUIDA, ISTRUZIONI OPERATIVE ED OBBLIGHI

Copia Numero: 01 Verificata da

Responsabile protezione dati

Rev.	Descrizione	Data	Firma
0	Prima redazione	14-05-2019	

INDICE

1 PREMESSA

La riservatezza delle persone attraverso la corretta acquisizione, gestione e circolazione dei dati personali e mediante l'adozione di adeguate misure di sicurezza per la loro protezione è tutelata dal Regolamento UE 2016/679 .

Il trattamento dei dati personali richiede obbligatoriamente l'adozione di idonee e preventive misure di sicurezza e che, chiunque essendovi tenuto omette di adottarle è suscettibile di sanzioni penali e civili. Le misure di sicurezza prescritte dal Reg. UE 2016/679 sono intese nel senso più ampio e riguardano il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali che configurano i livelli di protezione necessari a ridurre al minimo i rischi di distruzione, perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Nell'ambito del più generale quadro degli obblighi di sicurezza, il Reg. UE 2016/679 prescrive in modo specifico le misure che debbono comunque essere adottate per assicurare un livello adeguato di protezione dei dati personali..

In ottemperanza agli obblighi di legge ed a garanzia della correttezza dei trattamenti effettuati sui dati personali, per i quali l'Azienda opera in qualità di Titolare del trattamento, viene emesso il seguente regolamento aziendale.

Tutto il personale dipendente e assegnati ad unità operative interne, i consulenti di aziende esterne o collaboratori autonomi, gli addetti alla manutenzione, le persone esterne dipendenti di altre ditte, sono tenuti a rispettarlo scrupolosamente, nell'ambito delle proprie competenze ed attività.

Il presente regolamento costituisce la disciplina aziendale per i trattamenti dei dati personali, con particolare riferimento alle misure di sicurezza poste a tutela dei trattamenti effettuati:

- con strumenti elettronici (prevalentemente: computer, sia operanti in modalità singola, sia in rete);
- senza l'ausilio di strumenti elettronici (prevalentemente: atti e documenti cartacei).

Le indicazioni di seguito riportate sono obbligatorie con decorrenza immediata ed hanno valore di ordine di servizio. La loro violazione, parziale o totale, potrà essere suscettibile di provvedimenti disciplinari commisurati alla gravità della violazione; pertanto, si prega di leggere con la massima attenzione le disposizioni di seguito enunciate.

Si dispone, inoltre, che:

- copia del regolamento venga consegnato, all'atto dell'assunzione o dell'avvio del rapporto di collaborazione, ad ogni nuovo dipendente o collaboratore interessato;
- i Responsabili delle Funzioni aziendali, ciascuno nell'ambito delle proprie competenze, provvedano a rendere esecutive le norme del presente regolamento e vigilino sulla costante applicazione ed il rispetto delle disposizioni impartite, riferendo al **Responsabile del Trattamento**;
- in caso di esigenze di chiarimento o di necessità di disposizioni, relativamente a normative ancora in preparazione, ovvero di segnalazione di episodi rilevanti in materia di sicurezza, gli incaricati debbono rivolgersi al proprio superiore gerarchico.

Ai fini del Regolamento UE 2016/679 si intende per:

1) **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;
2) **Dati genetici**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
3) **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;
4) **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;
5) **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;
6) **Limitazione di trattamento**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
7) **Profilazione**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
8) **Pseudonimizzazione**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile
9) **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;
10) **Titolare del trattamento**: 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;

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

12) **Responsabile della Protezione dei Dati (DPO)**: persona fisica o giuridica, designata dal Titolare del trattamento e dal Responsabile del trattamento, incaricata di sorvegliare l'osservanza del Regolamento UE 2016/679 in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

13) **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; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

14) **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;

15) **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;

16) **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;

17) **Rappresentante**: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) **Impresa**: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) **Gruppo imprenditoriale**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) **Norme vincolanti d'impresa**: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) **Autorità di controllo**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) **Autorità di controllo interessata**: un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che

risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;

23) **Obiezione pertinente e motivata**: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

Nell'ambito dell'organizzazione del lavoro, ai soli fini degli adempimenti di legge, i dati personali oggetto di trattamento vengono divisi in relazione alla loro natura in due principali classi:

1. la prima classe riguarda i **dati personali** e comprende i dati relativi ai clienti, dipendenti, consulenti e fornitori, e comunque oggetto di trattamento (sia se riferiti a soggetti giuridici, sia se riferiti a soggetti fisici);
2. la seconda classe riguarda le eventuali **categorie particolari di dati personali Capo II art.9 "***dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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"*relative ai consulenti, ai dipendenti, ed ai propri familiari; in questa classe rientrano anche gli eventuali dati personali dei clienti, dagli stessi definiti tali ai sensi della normativa.

2 INCARICATI DEL TRATTAMENTO

Ai sensi dell'art.29 del Regolamento UE 2016/679 il personale dipendente è incaricato di trattare i dati personali necessari per lo svolgimento delle funzioni ad esso collettivamente affidate e di compiere le sole operazioni di trattamento a ciò strumentali, attenendosi alle istruzioni contenute nel presente documento, o impartite nel corso dell'attività e rispettando le pertinenti disposizioni contenute in specifiche comunicazioni interne.

"*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".*

Gli incaricati potranno accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti a ciascuno assegnati.

Gli incaricati, nel trattare i dati personali, dovranno operare garantendo la massima riservatezza delle informazioni di cui vengono in possesso, considerando tutti i dati personali confidenziali e, di norma, soggetti al segreto d'ufficio; è fatta eccezione per i soli dati anonimi, generalmente trattati per elaborazioni statistiche, e quelli acquisibili da chiunque perché contenuti in atti, liste ed elenchi pubblici seguendo in tal caso comunque gli obblighi di legge. I dati personali non potranno essere trasmessi a terzi, esterni, se non espressamente autorizzato dalla Direzione aziendale.

La procedura di lavoro e la condotta tenuta nello svolgimento delle operazioni di trattamento, dovranno evitare che:

- i dati personali siano soggetti a rischi di distruzione e perdita anche accidentale;
- ai dati possano accedere persone non autorizzate;
- vengano svolte operazioni di trattamento non consentite o non conforme ai fini per i quali i dati sono stati raccolti.

Gli incaricati dovranno perciò operare con la massima diligenza ed attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, all'eventuale loro aggiornamento, così per la conservazione ed eventuale cancellazione o distruzione.

Gli incaricati non potranno eseguire operazioni di trattamento per fini non previsti tra i compiti loro assegnati dai diretti responsabili o superiori e comunque riferiti alle disposizioni e regolamenti vigenti in Azienda.

Gli incaricati non potranno, di propria iniziativa, iniziare nuovi trattamenti, attivare nuove procedure informatiche per la gestione od elaborazione di dati personali, archivi cartacei o file di persone fisiche o giuridiche. Non potranno altresì essere fatte copie di archivi di dati, in tutto od in parte, se non espressamente richiesto per l'esecuzione delle proprie mansioni, e comunque su supporti che diano adeguate garanzie di sicurezza.
L'incarico viene conferito ai dipendenti in relazione alla natura dei trattamenti da loro svolti, alle modalità di trattamento ed ai mezzi utilizzati nell'ambito dei trattamenti previsti dalla unità operativa di appartenenza.
L'incarico viene correlato ai compiti ed alle funzioni svolte in modo tale da poter raggruppare, per classi omogenee di comportamento, uniformi profili di autorizzazione al trattamento, a loro volta rapportati ai profili di autorizzazione per l'accesso ai dati ed ai relativi trattamenti con strumenti elettronici.

2.1 Ambito del trattamento consentito

I dati personali, definiti nella pagina precedente, potranno essere trattati esclusivamente dagli Operatori dell'ufficio Amministrazione e Sicurezza sul lavoro, nonché dai diretti superiori. Taluni incaricati di trattamenti di dati personali potranno ricevere ulteriori specifiche indicazioni che integrano quelle generali di cui al presente Documento.
Le nomine ad incaricato sono estese, con analoghi criteri e modalità, anche ai non dipendenti, ed in particolare a quelle persone che funzionalmente svolgono operazioni di trattamento su dati di cui l'Azienda ha la titolarità. In questa classe di incaricati sono stati raggruppati i consulenti di aziende esterne o collaboratori autonomi limitatamente al periodo di collaborazione.

2.2 Lista degli incaricati ed aggiornamento dell'ambito del trattamento

Il Responsabile del trattamento compila in formato elettronico, aggiorna e conserva una lista degli incaricati per il trattamento di dati di cui *l'Azienda* è Titolare *(*comprendente l'ambito del trattamento riservato a ciascun incaricato, specificando quali categorie di dati personali tratta l'incaricato.

La lista è compilata specificando i trattamenti svolti dai singoli incaricati (o in aree omogenee di incarico) mediante strumenti elettronici oppure su atti e documenti cartacei. Periodicamente,

con cadenza almeno annuale, lo stesso Ufficio verifica la sussistenza delle condizioni per la conservazione dei profili di autorizzazione da parte degli incaricati.

La lista degli incaricati e l'ambito del trattamento consentito è correlata ai singoli profili di accesso alla rete informatica aziendale. Gli incaricati hanno accesso ai soli dati necessari per lo svolgimento delle loro attività.

Il responsabile del trattamento adotta tutte le misure di sicurezza richieste ai sensi dell'art. 32 del Regolamento, e tiene un **Registro delle attività di trattamento** svolte sotto la propria responsabilità. Tale registro contiene le seguenti informazioni:

- Il nome e i dati di contatto del titolare del trattamento;
- Le finalità del trattamento;
- Una descrizione delle categorie di interessati e delle categorie di dati personali;
- Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati.

Il registro contiene inoltre le seguenti informazioni, ove applicabile:

- I termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- Una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32, par. 1 del Regolamento.

3 LE MISURE DI SICUREZZA

Il Regolamento UE 2016/679 prescrive all'art. 32 l'obbligo di custodire e controllare i dati personali oggetto di trattamento "anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento".

Tale obbligo, posto a carico del Titolare dei dati, è rivolto a ridurre al minimo i rischi di distruzione o perdita, di accesso non autorizzato o trattamento non consentito dei dati.

Per il generale adempimento di tali prescrizioni e per conseguire in ogni caso il migliore livello di protezione dei dati personali trattati, sono adottate e prescritte le misure di sicurezza illustrate nei paragrafi che seguono.

*E' fatto obbligo ad ogni incaricato di adottare ed osservare scrupolosamente le misure di sicurezza prescritte dal Regolamento, sia in relazione alla loro natura di ordine di servizio aziendale, sia in relazione alle responsabilità personali previste dal sistema sanzionatorio del "*Regolamento UE 2016/679 art.83 *".*

Il Regolamento prescrive all'art. 32 le misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio:

- La pseudonimizzazione e la cifratura dei dati personali;
- La capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Si intende per:

“misure di sicurezza”, il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
"strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
"autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
"credenziali di autenticazione", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
"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 delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i 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.

4 NORME PER I TRATTAMENTI SVOLTI CON STRUMENTI ELETTRONICI

La presente sezione del regolamento aziendale comprende le istruzioni operative generali relative ai trattamenti svolti con strumenti elettronici .

Sistema di autenticazione informatica

- Autenticazione informatica
- Procedura di gestione delle credenziali di autenticazione
  - ✓ Parola chiave
  - ✓ Codice identificativo personale
- Protezione della postazione di lavoro
- Disposizioni per assicurare la disponibilità di dati o strumenti elettronici in caso di assenza o impedimento dell’incaricato

Sistema di autorizzazione;

Altre misure di Sicurezza;

- Aggiornamento dell’ambito di trattamento
- Antivirus e protezione da programmi pericolosi
- Procedure di aggiornamento dei programmi per elaboratore per prevenire vulnerabilità e correggere difetti
- Procedura per la custodia di copie di sicurezza

Ulteriori misure in caso di trattamento di categorie particolari di dati personali

- Protezione dalle intrusioni e dagli accessi abusivi
- Custodia e riutilizzo dei supporti
- Ripristino dell’accesso ai dati

Ulteriori misure di sicurezza

- Licenze d'uso dei programmi software
- Internet e posta elettronica
- Conversazioni telefoniche
- Viva voce
- Fax
- Autorizzazioni all'ingresso nei locali e controllo accesso ai locali
- Videosorveglianza
- Trattamento in rete per fini personali (se organizzati in banche dati).

4.1 Sistema di Autenticazione informatica

4.1.1 Autenticazione informatica

1.Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

Il trattamento di dati personali con strumenti elettronici di cui l'Azienda ha la titolarità, è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato (UserId) associato a una parola chiave (Password) riservata, conosciuta solamente dall'interessato.

4.1.2 Procedura di gestione delle credenziali di autenticazione

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Ad ogni incaricato possono essere assegnate più credenziali di autenticazione per l'accesso ai sistemi aziendali.

In caso di non utilizzo delle credenziali per un periodo predefinito e comunque non oltre i 6 mesi, oppure in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali, le stesse credenziali sono disattivate.

Fanno eccezione le credenziali assegnate e preventivamente autorizzate per finalità di gestione tecnica e di emergenza dei sistemi.

4.1.2.1 Parola chiave

I computer aziendali resi disponibili agli incaricati del trattamento ed agli addetti alla manutenzione HW e SW, sono sia fissi, che da tavolo *(desktop)* e possono essere connessi alla rete aziendale - stabilmente o temporaneamente - e/o alla rete internet.

Per l'uso dei computer, per l'accesso ai dati ed alla rete, è, tra l'altro, obbligatorio:

- per i PC che operano esclusivamente in modalità non connessa a rete*:* l'uso di una parola chiave*;*
- per i PC connessi in rete: l'uso di una parola chiave, di un codice identificativo personale per l'accesso ai dati, di un programma antivirus.

La parola chiave per l'accesso alla rete è personale e, come tale, non potrà essere comunicata ad altri soggetti, fatta eccezione per gli incaricati alla custodia delle medesime seguendo le regole di seguito impartite. Non potrà essere trascritta o annotata in maniera visibile da altri.

Ogni computer e il sistema prevedono la possibilità di utilizzare diverse parole chiave:

1. di *BIOS* all'accensione dello strumento (ove previsto),
2. di rete, che viene digitata sulla stessa maschera di ingresso insieme al codice identificativo personale,
3. di accesso alla rete interna aziendale (tipo LAN),

4. di protezione dello schermo video (*screen saver),*
5. di accesso diretto a specifici programmi software,
6. di accesso alla casella di posta elettronica *(e-mail),*
7. di accesso ad internet.

Ogni incaricato, per gli accessi di sua competenza, deve usare parole chiave diverse tra loro, ad eccezione dei punti 2, 3, 4 e 6 che obbligatoriamente assumono lo stesso valore.

Per i trattamenti in rete dovranno essere rispettate le direttive emesse al riguardo, tramite i canali di comunicazione aziendali (comunicati, normative, posta elettronica, ecc).

La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. **In caso di trattamento di dati particolari e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi**.

Le parole chiave ed codici identificativi adottati per l'accesso agli strumenti elettronici non possono essere usati per accedere ad altre banche dati esterne.

4.1.2.2 Codice Identificativo Personale

Tutti gli Incaricati che svolgono operazioni di trattamento di dati personali accedendo a computer connessi in rete sono dotati di un codice identificativo personale (UserID) univoco che non può essere assegnato a utenti diversi neppure in tempi diversi.

L'attribuzione di tale codice avviene secondo le regole in uso, previste dai gestori dei sistemi di sicurezza della rete:

- a ciascun dipendente è assegnato un codice identificativo (profilo) univoco per l'accesso alla rete.

4.1.3 Protezione della postazione di lavoro

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

È fatto obbligo di non lasciare incustodito ed accessibile lo strumento elettronico durante una sessione di trattamento. All'uopo si dovranno adottare le seguenti misure:

- Nel caso di abbandono temporaneo del posto di lavoro deve essere seguita la seguente procedura: digitare contemporaneamente i tasti **Alt+Ctrl+Canc**, premere il tasto **Invio**. A questo punto il PC è bloccato. Per sbloccarlo premere contemporaneamente i tasti **Alt+Ctrl+Canc**, inserire la propria password di rete e quindi digitare il tasto **Invio**.

Si rammenta inoltre che, ai fini di un'adeguata riservatezza dei dati nel corso dei trattamenti, dovrà essere attivato uno *screen saver* protetto da password ogni qual volta venga lasciato incustodito il proprio P.C.

4.1.4 Disposizioni per assicurare la disponibilità di dati o strumenti elettronici in caso di assenza o impedimento dell'incaricato

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

In caso di assenza o impedimento dell'incaricato, l'Azienda potrebbe trovarsi nella circostanza di dover accedere allo strumento o ai dati trattati dalla persona assente. Per tali motivi le parole chiave autonomamente sostituite da ciascun incaricato dovranno essere conservate e custodite nel rispetto delle modalità di conservazione cartacea.

1) La modalità di conservazione cartacea riguarda le seguenti categorie di incaricati:

A. Incaricati di trattare dati particolari;

B. Incaricati autorizzati al trattamento di dati personali residenti su P.C.

Ciascuno dei predetti soggetti, appena digitata la nuova password, sulla base dei criteri previsti nel regolamento aziendale, dovrà:

- scriverla sul modulo predisposto dall'azienda o, in mancanza di esso, su foglio bianco insieme al proprio nome, cognome e numero di matricola;
- inserire il foglio in una busta, chiudere ed incollare la busta, firmare sui margini di chiusura della busta, quindi applicare sulla chiusura stessa del nastro adesivo trasparente;
- scrivere il cognome, nome e numero di matricola in stampatello sulla busta, con l'indicazione, ove possibile, del codice identificativo del terminale;
- consegnare la busta all'Incaricato preposto alla custodia delle parole chiave.

Tutte le buste sigillate verranno custodite dal preposto alla custodia delle parole chiave, in un plico anch'esso chiuso, sigillato e riposto in un armadio o cassettiera chiuso a chiave.

Ove per ragioni organizzative sia necessaria la conoscenza di una parola chiave è prevista l'apertura della singola busta, alla presenza di terzi e con annotazione scritta dell'evento, rubricando anche l'ora e la data; dopo tali operazioni la password dovrà essere sostituita;

4.2 Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

L'ambito dei trattamenti automatizzati previsti per ciascun incaricato è correlato ai compiti ed alle funzioni svolte nella unità organizzativa di assegnazione e da luogo all'assegnazione di un profilo di autorizzazione al trattamento di dati personali. Tali profili sono organizzati per classi omogenee di comportamento e configurati anteriormente all'inizio del trattamento in maniera tale da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento nell'ambito assegnato all'incaricato. Annualmente deve essere verificato che i soggetti che accedono ai dati abbiano conservato le stesse qualità che consentono l'accesso. Di seguito, vengono riportate le regole dei diversi ambienti.

4.2.1 Autorizzazioni agli addetti alla manutenzione

I soggetti addetti alla manutenzione di elaboratori o P.C. sono autorizzati a svolgere le operazioni di manutenzione attenendosi alle disposizioni scritte sulla sicurezza di cui al presente regolamento.
Nel caso la manutenzione si riferisca a guasti e non ad aggiornamenti del software, per ogni elaboratore ed indipendentemente dalla loro connessione alla rete, ove si renda necessaria la rimozione di dischi, memorie o supporti magnetici per essere trasportati in laboratori esterni, l'addetto alla manutenzione ed il personale dipendente dovranno rispettare i comportamenti previsti per tali eventi, evitando di svolgere trattamenti non consentiti dei dati, anche considerando le restrizioni di cui alla successiva norma sul "riutilizzo controllato dei supporti".

4.3 Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. 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 da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

4.3.1 Aggiornamento dell'ambito del trattamento

Per quanto riguarda i dati di proprietà *dell'Azienda.* si fa riferimento al paragrafo 2.2.

4.3.2 Antivirus e protezione da programmi pericolosi

Su tutti i computer dell'azienda connessi in rete internet è installato un antivirus che viene aggiornato almeno ogni sei mesi. L'antivirus è installato in modalità residente in memoria e risulta, perciò, sempre attivo.

L'aggiornamento degli antivirus sono scaricate da internet dagli Operatori sul proprio P.C. connesso alla rete;

Mentre il Responsabile del Trattamento provvede a duplicare le versioni stesse su supporti magnetici da utilizzare per l'aggiornamento del software antivirus installato sui P.C. non connessi ad internet.

4.3.3 Aggiornamento periodico dei programmi per elaboratore finalizzato alla prevenzione delle vulnerabilità e alla correzione dei difetti

Il Responsabile del Trattamento dovrà provvedere tempestivamente ad eseguire le operazioni di aggiornamento, anche sulla base degli aggiornamenti predisposti dai fornitori dei sistemi software installati sugli strumenti utilizzati, al fine di evitare le vulnerabilità e correggere i difetti. Tale aggiornamento è obbligatorio almeno una volta all'anno; per i sistemi che consentono il trattamento di dati personali almeno semestralmente.

4.3.4 Procedura per la custodia di copie di sicurezza

Le funzioni competenti provvedono al backup periodico dei dati, secondo gli standard stabiliti avendo cura della conservazione in sicurezza delle copie di backup.

La copia dei dati registrati sui PC deve essere di routine e l'archiviazione dei supporti di backup deve avvenire in luogo sicuro e, ove possibile, distante dal computer per evitare che eventi disastrosi possano contemporaneamente danneggiare originali e copie dei dati trattati.

I dati contenuti su eventuali PC portatili, in funzione della loro importanza, sono sottoposti ad un salvataggio preventivo su un supporto adeguato con cadenza almeno mensile, allo scopo di evitarne la perdita anche se accidentale.

4.4 Registri delle attività di trattamento (applicabile in quanto l'Azienda tratta categorie particolari di dati personali come descritti all'Art. 9 del Reg. UE 679/2016)

19.1.Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
a)il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali; 4.5.2016 L 119/50 Gazzetta ufficiale dell'Unione europea IT
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

19.2.Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:
a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
19.3.I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.
19.4.Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.
19.5.Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

Il Responsabile del Trattamento, anche attraverso il coinvolgimento delle altre funzioni aziendali, cura l'aggiornamento dei Registri delle Attività di Trattamento.

4.5 Ulteriori misure in caso di trattamento di categorie particolari di dati personali

20. I dati di categorie particolari di dati personali sono protetti contro l'accesso abusivo, mediante l'utilizzo di idonei strumenti elettronici.

21. 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 e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati personali di categorie particolari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

4.5.1 Protezione dalle intrusioni e dagli accessi abusivi di cui all'art. 615-ter del codice penale

Gli elaboratori connessi alla rete internet sono configurati secondo lo standard aziendali, i sistemi anti intrusione sono costituiti da sistemi che garantiscono l'accesso alle risorse di rete da parte delle utenze all'uopo autorizzate. Ogni tentativo di accesso non autorizzato viene registrato sui log di sistema.

4.5.2 Custodia e riutilizzo dei supporti

Gli incaricati debbono custodire e controllare i supporti sui quali sono registrati i dati personali in maniera tale che soggetti non autorizzati non possano venire a conoscenza nemmeno

accidentalmente dei contenuti di tali supporti. I supporti, al termine di ogni lavorazione dovranno essere custoditi riposti in contenitori, armadi o cassetti muniti di serratura e chiusi e chiave.

Tali supporti non potranno essere utilizzati da altri soggetti che non possiedono l'incarico di poter trattare i dati in essi registrati.

In caso di cattivo funzionamento del supporto che ne determini l'impossibilità della lettura dei dati registrati, i supporti dovranno essere distrutti.

4.5.3 Ripristino dell'accesso ai dati

In caso di danneggiamenti che dovessero interessare dati personali ovvero gli strumenti che li contengono, le funzioni competenti e le società esterne utilizzate, assicurano il ripristino dell'accesso a tali dati in tempi certi compatibili con le esigenze di utilizzo degli utenti interessati e comunque non superiori ai sette giorni.

4.6 Ulteriori misure di sicurezza

4.6.1 Licenze d'uso dei programmi software

E' fatto divieto di installare ed usare programmi software non rilasciati ufficialmente dall'azienda e preventivamente testati circa la loro integrità.

4.6.2 Internet e posta elettronica

La connessione ad Internet deve avvenire solo per finalità professionali. Per motivi di sicurezza è sconsigliato il collegamento ad Internet attraverso connessioni effettuate via modem mediante le normali linee telefoniche (DialUp), salvo casi di provata necessità e preventivamente autorizzati.

Non è consentito importare programmi (anche *freeware*) o file di qualsiasi natura da Internet se non per uso professionale attinente le funzioni svolte e, comunque, solo previa notifica all'incaricato che gestisce il sistema.

Non sono consentiti l'apertura e l'esecuzione di file ricevuti in *e-m*ail da mittenti sconosciuti.

Non è consentito l'uso di Internet per la ricezione di programmi radio e musicali, per conversazioni in *chat line* o collegamenti con *webcam,* ad eccezione di straordinari motivi professionali (videoconferenze).

Le caselle di posta elettronica sono messe a disposizione per usi professionali, l'utilizzo personale comporta l'assunzione diretta di responsabilità sui contenuti dei messaggi da parte di chi li invia. Non è consentito inviare informazioni confidenziali tramite posta elettronica.

4.6.3 Conversazioni telefoniche

Non è consentito fornire informazioni particolari che impegnano l'Azienda, o sulle attività svolte, se non si è certi di chi sia l'interlocutore.

Spie industriali, pirati informatici (cracker) e altre persone che vogliono accedere ai sistemi aziendali spesso si camuffano per venire a conoscenza di numeri telefonici interni, password, nomi di collaboratori, ecc. A questa pratica viene dato il nome di "ingegneria sociale". Tutte le informazioni, anche se in apparenza irrilevanti, possono essere usate per organizzare un attacco informatico ai sistemi aziendali. Si eviti, quindi, di fornire telefonicamente informazioni sull'organizzazione interna a sconosciuti.

4.6.4 Viva voce

Nel caso la conversazione telefonica venga svolta in modalità "viva voce", l'interlocutore dovrà essere informato circa l'eventuale presenza di altri ascoltatori.

4.6.5 Fax

Usare la dovuta cautela nell'invio informale di messaggi fax, il loro contenuto potrebbe essere considerato come una formale comunicazione. Nell'invio di un fax contenente dati personali ad una persona autorizzata a visionarli, si inviti la persona destinataria ad essere vicina all'apparecchiatura ricevente al momento della ricezione.

4.6.6 Videosorveglianza (Impianti audiovisivi e altri strumenti di controllo)

Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali.
La disposizione non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. Le informazioni raccolte sono utilizzabili a tutti i fini connessi ala rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal Regolamento.

4.6.7 Autorizzazioni all'ingresso nei locali e controllo dell'accesso ai locali.

L'ingresso nei locali è riservato alle persone autorizzate. Sono permanentemente autorizzati: i dipendenti, i consulenti, gli addetti alla manutenzione (relativamente ai soli luoghi necessari allo svolgimento delle loro attività).

All'interno degli uffici possono accedere stabilmente solo le persone autorizzate, nel caso di presenza occasionale di altri soggetti, il personale autorizzato ai trattamenti opererà in maniera da **non consentire la conoscenza di dati personali** agli altri soggetti occasionali.

4.6.8 Misure in caso di "Cessazione del rapporto di lavoro"

Nel caso di cessazione del rapporto di lavoro è prevista la restituzione da parte dell'incaricato degli strumenti assegnatigli dall'azienda (es: PC portatile aziendale, cellulare di servizio, etc.). Il Responsabile del Trattamento provvederà alla formattazione delle unità disco rigido associate al PC portatile ed eventuali periferiche di archiviazione aggiuntive, con conseguente distruzione di tutti gli eventuali riferimenti a dati personali e/o sensibili, provvedendo inoltre all'azzeramento della memoria del telefono cellulare con conseguente eliminazione di tutti i dati in essa presenti.

4.6.9 Trattamento in rete per fini personali (se organizzati in banche dati)

Il trattamento per fini esclusivamente personali, effettuato mediante i P.C. in dotazione, di dati personali ordinari e/o particolari, organizzati in banche dati e registrati sul disco rigido del P.C., non è consentito.

Non sono, comunque, consentiti trattamenti per fini personali dei dati in possesso dell'Azienda.

5 NORME PER I TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Di seguito sono indicate le azioni di sicurezza nel caso di trattamenti di dati personali senza l'ausilio di strumenti elettronici, e quindi con modalità essenzialmente manuali e cartacee.

Sono a tale proposito adottate in azienda le seguenti misure organizzative e procedurali, che oltre ad adempiere ai livelli minimi previsti dalla legge, hanno l'obiettivo di assicurare una migliore e più ampia tutela dei documenti e dei dati personali in essi contenuti.

La presente sezione di regolamento aziendale comprende le istruzioni operative generali relative a:

Aggiornamento periodico dell'ambito di trattamento consentito
Custodia e controllo di atti e documenti

- Accesso ai soli dati necessari
- Conservazione in archivi ad accesso selezionato
- Restituzione atti e documenti al termine delle operazioni

Accesso controllato agli archivi

- Identificazione e registrazione dei soggetti ammessi agli archivi

Ulteriori misure di sicurezza

- Custodia e conservazione delle riproduzioni
- Distruzione di documenti cartacei

5.2 Aggiornamento periodico dell'ambito di trattamento consentito

24. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

5.3 Custodia atti e documenti e conservazione in archivi.

25. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

Gli atti e i documenti, di qualunque natura, devono essere trattati con diligenza, custoditi e conservati in maniera che le persone non incaricate non possano venirne a conoscenza. Gli atti e documenti contenenti dati personali debbono comunque essere conservati in archivi che consentano sempre, in caso di ricerche, l'accesso selezionato ai dati.
La loro l'archiviazione dovrà quindi essere effettuata a mezzo di cartelle, classificatori, schedari o altri contenitori, ordinati per argomento, tipologia, o altre caratteristiche omogenee e sulla base di criteri alfabetici, cronologici o di altra natura, tali comunque da consentirne il reperimento sulla base di specifici parametri di ricerca che evitino la consultazione di dati non attinenti al compito da svolgere.

Gli incaricati abilitati al trattamento di dati provenienti (o direttamente tratti) da archivi ad accesso selezionato, devono conservare e custodire i dati trattati con la massima riservatezza evitando che vengano volontariamente o involontariamente conosciuti da soggetti privi della stessa qualificazione di incaricato o che abbiano incarichi di diversa ampiezza.

L'accesso agli archivi contenenti atti e i documenti di dati personali di qualunque natura è riservato alle sole persone incaricate ed autorizzate a potervi accedere. L'autorizzazione generale riguarda tutte le persone che operano con la qualificazione di incaricato, limitatamente ai settori aziendali nei quali, di norma, sono assegnati, quindi, agli archivi delle singole funzioni aziendali possono accedere solo le persone incaricate di svolgere attività in quegli ambienti.

5.3.1 Accesso ai soli dati necessari

Durante lo svolgimento di trattamenti di dati personali di qualunque natura, registrati su carta o altri supporti non informatici, i singoli incaricati delle diverse operazioni di trattamento devono operare in maniera da svolgere le operazioni di trattamento solo su quei dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti previsti per le specifiche attività attribuite alla funzione ricoperta. E' pertanto vietata ogni forma di trattamento di dati personali non pertinente con le finalità lavorative aziendali.

5.3.2 Restituzione atti e documenti al termine delle operazioni

Gli atti e i documenti devono essere trattenuti solo per il periodo strettamente necessario allo svolgimento delle operazioni inerenti ai propri compiti e al termine delle operazioni devono

essere restituiti o riposti nell'archivio dal quale erano stati prelevati (o presso il quale devono essere custoditi).

5.4 Accesso controllato agli archivi

26. L'accesso agli archivi è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

L'accesso agli archivi contenenti atti e documenti di dati particolari ovvero di dati personali, viene controllato dallo stesso personale Incaricato di trattare tali dati, seguendo le apposite disposizioni impartite dal responsabile della funzione.

5.5 Ulteriori Misure di Sicurezza

5.5.1 Identificazione e registrazione dei soggetti ammessi agli archivi dopo l'orario di chiusura

Le persone che accedono agli archivi contenenti atti e documenti di dati personali ovvero dei dati personali aziendali, dopo l'orario di chiusura, devono essere preventivamente autorizzati dalla Direzione aziendale.

5.5.2 Custodia e conservazione delle riproduzioni

I supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali sensibili e giudiziari ovvero di dati personali, devono essere custoditi e conservati con le stesse modalità previste dal regolamento aziendale, nei punti precedenti, per i trattamenti degli atti e i documenti originali.

5.5.3 Distruzione di documenti cartacei

Nel caso di distruzione di documenti contenenti dati personali di qualsiasi natura, sia comuni sia di tipo sensibile e giudiziario, l'Incaricato deve curare che i dati in questione non possano venire a conoscenza di persone che non abbiano la stessa qualifica di Incaricato predisponendoli in maniera opportuna.

Pertanto i documenti andranno distrutti singolarmente, mentre eventuali tabulati risultanti da trattamenti automatizzati, dovranno essere riposti in scatoloni chiusi con nastro adesivo e con l'indicazione all'esterno dello scatolone di **"a distruzione riservata"**, in maniera da garantirne la riservatezza per il successivo processo di distruzione effettuato dal personale addetto a tale incombenza.

5.5.4 Verifiche e Controlli periodici

Si informa, infine, che il Titolare del trattamento potrà disporre verifiche e controlli periodici circa la puntuale osservanza delle disposizioni di cui al presente regolamento.