REGISTRO DEI TRATTAMENTI DEI DATI PERSONALI

FELCARO

FELCARO S.a.s. di Felcaro Mauro & C.
Via Divisione Julia, 25/1
33044 MANZANO (UD)

INDICE

Parte I – ANALISI DELLA SITUAZIONE DELL'ENTE

1) - Anagrafica dell'Ente

Identificazione Ente	**FELCARO S.a.s. di Felcaro Mauro & C.** **Via Divisione Julia, 25/1** **33044 MANZANO (UD)**
Partita I.V.A. e C.F.	IT01906270309
Codice ISTAT/ATECO	71.1 – attività degli studi di architettura, ingegneria ed altri studi tecnici
Descrizione attività	La società ha per oggetto la prestazione di servizi di consulenza tecnico, industriale, gestionale e direzionale a diverse tipologie di aziende, a lavoratori autonomi o a terzi. Le attività vengono svolte negli uffici della sede.
Titolare Trattamento Dati (TTD)	Felcaro Mauro
Responsabile Protezione Dati (RPD-DPO)	Non Applicabile
Amministratore Sistema (AS)	Felcaro Mauro
Addetto Trattamento Dati (ATD)	Vedi tabelle a seguire
Responsabile Trattamento Esterno (RTE)	Vedi tabelle a seguire
Consulente al Titolare Trattamento Dati	Felcaro S.a.s. di Felcaro Mauro & C. Via Divisione Julia, 25/1 - 33044 MANZANO (UD) Tel. 0432/755188 – e mail: info@felcaro.it – Fax 0432/741774

2) - Distribuzione dei compiti e delle responsabilità nella struttura dell'Ente

Addetti Trattamento Dati:

Cognome e Nome	Indirizzo	Mansione
Braida Giulia	Via Don Dante Silvestri, 10 33044 MANZANO	Impiegata
Trinco Sonia	Via del Lof, 45 33043 CIVIDALE DEL FRIULI	Impiegata

Responsabili Esterni Trattamento:

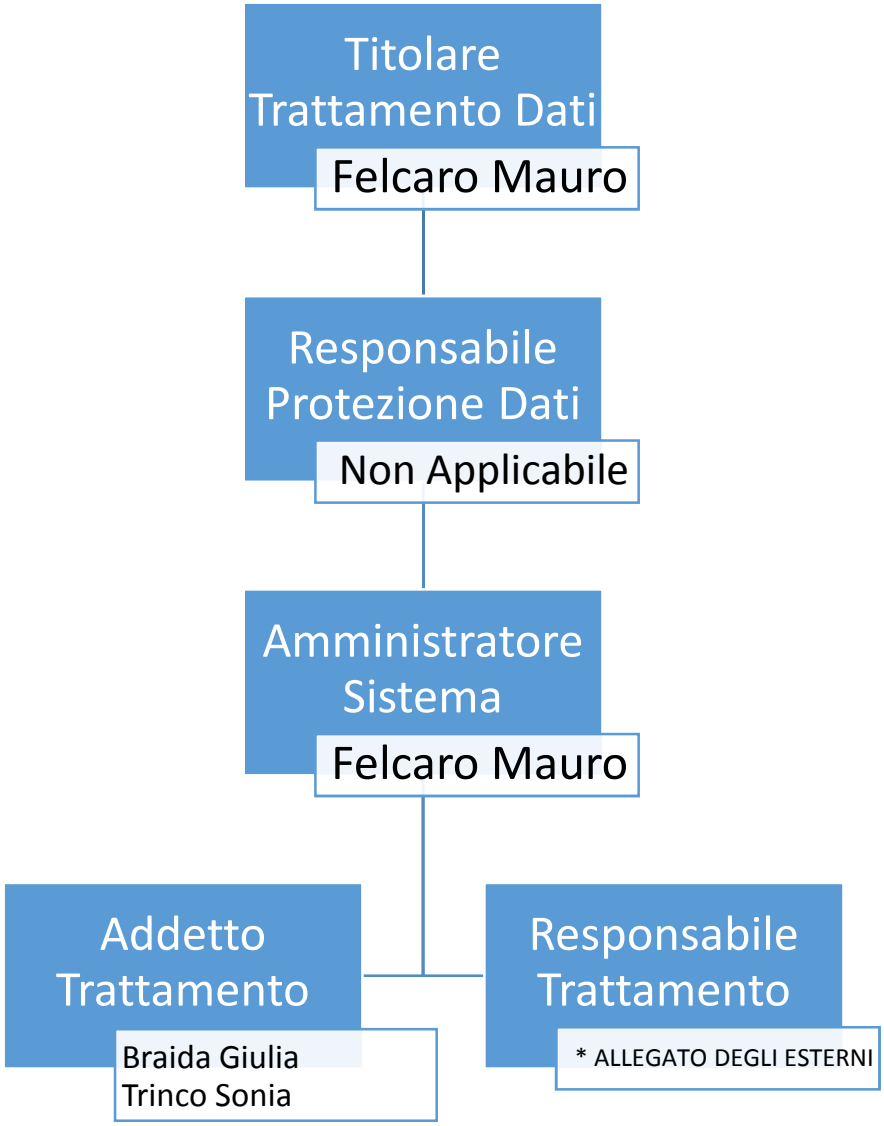
Cognome e Nome / Ragione sociale	Indirizzo	Mansione
Molinari Stefania S.r.l.	Via Piemonte, 50/4 33100 UDINE (UD)	Medico Competente - Struttura organizzativa di medicina del lavoro
Sassara Dott. Stefano	Viale Giovanni Paolo II, 15/4 33100 UDINE (UD)	Consulente del lavoro
Studio Commercialisti Associati Dott. Mario Nobile e Dott.ssa Francesca Vidal	Via Divisione Julia, 54 33044 MANZANO (UD)	Consulente fiscale
Infoserver S.n.c. di Gallo Nicola e Fogar Alessandro	Via Trieste, 9/5 33044 MANZANO (UD)	Consulente informatico
Elmas Software S.p.a.	Via Delle Crede, 4/B 33170 PORDENONE (PN)	Consulente informatico
Mestieri & Mestieri Soc. Coop.	Via Cussignacco, 78/4 33040 PRADAMANO (UD)	Impresa di pulizie

Le banche dati su supporti informatici e/o cartacei sono le seguenti:

- programmi, moduli e registri della contabilità generale e fiscale;
- programmi, moduli e registri della gestione del personale e paghe;
- programmi, moduli e registri dei controlli medico sanitari;
- programmi, moduli e registri per le attività di sicurezza sul lavoro;
- altri.

In questo ruolo e nei limiti delle mansioni affidate, potranno eseguire le operazioni di trattamento riguardanti le sopraddette banche dati, attenendosi alle istruzioni impartite dal Titolare del Trattamento Dati.
In particolare, in riferimento alla sicurezza del trattamento dei dati secondo il Regolamento europeo 2016/679, vengono fornite, le istruzioni operative che avranno cura di osservare con la dovuta attenzione, consapevoli che la loro scrupolosa applicazione è condizione necessaria per non vanificare le misure e le procedure implementate dalla società nel campo della sicurezza del trattamento dei dati personali.
Nel singolo documento di nomina allegato, sono evidenziate le operazioni riguardanti il trattamento di dati personali di propria competenza e le banche dati a cui il singolo incaricato può accedere. Inoltre, gli Incaricati al Trattamento quando procedono alla raccolta dei dati personali e/o particolari dei dipendenti e/o collaboratori, o di terzi soggetti, nel corso della normale attività operativa dell'ente, devono rilasciare l'informativa ed il modulo per la raccolta del consenso al trattamento dei dati, al fine di ottenere l'autorizzazione a mezzo firma al trattamento degli stessi, in base a quanto citato nell'informativa.

3) - Organigramma dell'Ente



4) - Finalità del documento e definizioni

Il presente Registro del Trattamento dei Dati Personali è redatto ai sensi dell'art.30 del Regolamento europeo 2016/679 del 27 aprile 2016 seguendo i 173 punti del "Considerando" e allegati.
Il Regolamento si pone come obbiettivo di realizzare un'informativa adeguata nei confronti dei dipendenti, dei collaboratori e delle parti interessate, sul corretto e diligente comportamento da adottare in merito al trattamento dei dati personali e/o dati particolari che rappresentano il patrimonio informativo della società, previsto dal "vecchio Codice della Privacy", sia mediante strumenti elettronici, sia mediante utilizzo di supporti cartacei, onde evitare di incorrere in sanzioni amministrative e penali.
Al fine di rendere più chiaro il significato della terminologia adottata nel Regolamento di Protezione dei Dati Personali di seguito vengono riportate le definizioni terminologiche più ricorrenti e importanti.

Banca dati: qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato in modo tale da facilitare il trattamento.

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme 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.

Titolare del trattamento: la persona fisica o la persona 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 determinate 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 e degli Stati membri.

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

Amministratore di sistema: la figura professionale, in ambito informatico, finalizzata alla gestione ed alla manutenzione di un impianto di elaborazione o delle sue componenti con cui vengono effettuati trattamenti di dati, compresi i sistemi di gestione di basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza.

Incaricato e/o addetto al trattamento: la persona fisica che effettua i trattamenti sui dati sulle basi di istruzioni scritte dal titolare o, se nominato, dal responsabile del trattamento.

Interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

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.

Dato particolare: dato personale che rilevi l'origine razziale o etnica, le convinzioni religiose o filosofiche, le opinioni politiche, l'appartenenza a 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.

Dato giudiziario: dato personale relativo alle condotte penali e ai reati o a connesse misure di sicurezza.

Comunicazione di dati personali: dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

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

Informativa: il Titolare deve sempre specificare i dati di contatto del RPD-DPO (Responsabile della Protezione dei Dati e/o del Data Protection Officer), qual è il suo interesse legittimo e se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).

Ulteriori informazioni "necessarie per garantire un trattamento corretto e trasparente" si deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.
Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Diritto di accesso: il diritto di accesso prevede in ogni caso il diritto di ricevere una copia dei dati personali oggetto del trattamento.

Diritto di limitazione: il diritto così detto "al blocco" del trattamento è esercitabile non solo in caso di violazione dei presupposti di liceità, bensì anche se l'interessato chiede la rettifica dei dati o si oppone al loro trattamento.

Diritto di cancellazione: il diritto così detto "all'oblio" si configura come diritto alla cancellazione dei propri dati personali. E' previsto anche l'obbligo del titolare (se ha reso ad altri i dati personali dell'interessato) di informare della richiesta di cancellazione altri titolari che trattano i dati dell'interessato.

Diritto alla portabilità: non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al titolare. Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di dati personale 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.

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.

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

Notifica della violazione dei dati personali: il titolare dovrà notificare all'Autorità di controllo le violazioni di dati personali di cui venga a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.
La notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo". I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del regolamento.
Il titolare di trattamento dovrà in ogni caso essere in grado di documentare le violazioni di dati personali subite.

5) – Risk Assessment

Durante i processi di "valutazione" e "gestione", i rischi vengono identificati valutando le situazioni operative, stimando le conseguenze che eventi indesiderabili potrebbero avere, prevedendo la possibilità che questi eventi accadano e soppesando il valore di ogni possibile conseguenza, programmare le misure di protezione.
La stima dei rischi è una linea di condotta durante la quale strategie diverse sono valutate e vengono prese decisioni sui rischi ritenuti accettabili. Queste strategie hanno differenti effetti sui rischi, inclusi la riduzione, la rimozione e la ridefinizione degli stessi. Alla fine, viene determinato un livello accettabile di rischio (rating 1) e di conseguenza viene adottata una strategia di mantenimento e monitoraggio continuo.

La seguente matrice illustra il metodo di lavoro adottato e la definizione dell'indice di rischio ipotizzato.

PROBABILITÀ \ GRAVITÀ				
	4	8	12	16
	3	6	9	12
	2	4	6	8
	1	2	3	4

R = PxG

Scala delle probabilità **P** di accadimento di un evento

VALORE	LIVELLO	DEFINIZIONI/CRITERI
4 CERT ALMOST	Quasi certo	Esiste una correlazione diretta tra la mancanza rilevata ed il verificarsi dell'evento ipotizzato. Sono noti episodi e eventi per la stessa mancanza, rilevati in ambienti simili o situazioni operative simili.
3 LIKELY	Probabile	La mancanza rilevata può provocare un evento, anche se non in modo automatico o diretto. E' già noto qualche episodio in cui alla mancanza rilevata ha fatto seguito l'evento.
2 UNLIKELY	Improbabile	La mancanza rilevata può provocare l'evento al contemporaneo verificarsi di particolari situazioni e condizioni. Sono noti solo rari episodi già verificatisi.
1 REMOTE	Remoto	La mancanza rilevata può provocare l'evento per concomitanza di più fatti poco probabili e indipendenti. Non sono noti episodi già verificatisi.

Scala dell'entità del gravità **G** di accadimento di un evento

VALORE	LIVELLO	DEFINIZIONI/CRITERI
4 SEVERE	Altamente probabile Catastrofico	Esiste una correlazione diretta tra la mancanza rilevata ed il verificarsi dell'evento ipotizzato. Sono noti episodi e eventi per la stessa mancanza, rilevati in ambienti simili o situazioni operative simili.
3 HIGH	Probabile Critico	La mancanza rilevata può provocare un evento, anche se non in modo automatico o diretto. E' già noto qualche episodio in cui alla mancanza rilevata ha fatto seguito l'evento.
2 MODERATE	Poco probabile Moderato	La mancanza rilevata può provocare l'evento al contemporaneo verificarsi di particolari situazioni e condizioni. Sono noti solo rari episodi già verificatisi.
1 LOW	Improbabile Insignificante	La mancanza rilevata può provocare l'evento per concomitanza di più fatti poco probabili e indipendenti. Non sono noti episodi già verificatisi.

R 16	Azioni correttive indilazionabili	PRIORITÀ P1
R 8 - 12	Azioni correttive da programmare con urgenza	PRIORITÀ P2
R 2 - 6	Azioni correttive e/o migliorative da programmare nel medio termine	PRIORITÀ P3
R 1	Azioni migliorative in fase di programmazione	PRIORITÀ P4

Range dei valori: Categoria di Rischio – Possibili Azioni

CATEGORIA	ENTITÀ	RIFERIMENTO GRIGLIA	PRIORITÀ DI AZIONE
R 16 P 1	ALTO	Altissima probabilità	Elevatissima probabilità che un evento accada, azione immediata al fine di ridurre il rischio. Area in cui individuare ed attuare miglioramenti con interventi di protezione.
R 8 – 12 P 2	MEDIO	Alta probabilità	Alta probabilità che un evento accada, azione immediata per ridurre il rischio. Area in cui individuare e programmare miglioramenti con interventi di protezione anche con azioni a lungo termine per ridurre la probabilità.
R 2 – 6 P 3	BASSO	Media probabilità	Probabilità che accada un evento, azioni di monitoraggio sul sistema. Eseguire un controllo standard per ridurre e mantenere la probabilità al livello più basso possibile.
R 1 P 4	TRASCURABILE	Bassa probabilità	Area in cui gli eventi potenziali sono sufficientemente sotto controllo. Eseguire un controllo periodico (ad es. annuale) per assicurare che la probabilità non aumenti.

6) - L'Analisi dell'Ente – Analisi del Rischio "main risk assessment"

N.	Requisito	Adeguato/Non Adeguato - Note			
		SI	NO	Risk Level	
1	L'organizzazione ha un numero di dipendenti pari o superiore a 250?		X	0	
2	Sono effettuati trattamenti che possono presentare un rischio per i diritti e le libertà degli interessati?	X		1	
3	Il trattamento di dati è occasionale?		X	3	
4	Il trattamento include "categorie particolari di dati di cui all'articolo 9, paragrafo 1 (che sono gli odierni dati particolari, con l'aggiunta dei dati genetici e biometrici), o i dati personali relativi a condanne penali e a reati di cui all'articolo 10"?	X		3	
5	Contiene il registro, il nome e i dati di contatto del titolare del trattamento?	X		1	
6	Sono indicati il nome e i dati di contratto, ove sussistenti: • del contitolare del trattamento? • del rappresentante del titolare del trattamento? • del responsabile della protezione dei dati?	X		1	
7	Sono esplicitate le finalità dei trattamenti effettuati?	X		1	
8	Per ciascun trattamento sono individuate le categorie di interessati (ad es., dipendenti, clienti/utenti, fornitori, ecc.)?	X		1	
9	Per ciascun trattamento sono individuate le categorie di dati, sono cioè rintracciati: • dati che rivelano l'origine razziale o etnica? • dati che rivelano le opinioni politiche? • dati che rivelano le convinzioni religiose o filosofiche? • dati che rivelano l'appartenenza sindacale? • dati genetici? • dati biometrici? • dati relativi alla salute? • dati relativi alla vita/orientamento sessuale? • dati relativi a condanne penali e reati?	X		1	
10	Per ciascun trattamento sono indicate le categorie di destinatari, cui i dati sono o saranno comunicati?	X		1	
11	Vi sono trattamenti in cui i dati sono comunicati a destinatari di Paesi terzi ovvero di organizzazioni internazionali?		X	0	
12	Contiene il registro l'indicazione dei trattamenti che includono i trasferimenti di dati personali verso un paese Terzo o un'organizzazione internazionale?		X	0	
13	Il registro include l'identificazione del paese terzo o dell'organizzazione internazionale?		X	0	
14	il registro documenta le prescritte garanzie adeguate che sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse? Se il registro è destinato a essere consultato da persone aventi un legittimo interesse, il trasferimento è ammesso soltanto su richiesta di tali persone o qualora tali persone ne siano i destinatari?		X	0	
15	E' individuata la base giuridica (ad es., contratto, legge, standard internazionale, ecc.) di ciascun trattamento?	X		1	
16	Detta base giuridica consente, per ciascun trattamento, di definire un tempo massimo di gestione/conservazione dei dati?	X		1	
17	Sono indicati i termini ultimi previsti per la cancellazione delle diverse categorie di dati?	X		1	
18	Sono descritte le misure di sicurezza tecniche e quelle organizzative a titolo di esempio: • 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?	X		1	
19	Dette misure garantiscono un livello di sicurezza adeguato al rischio?	X		1	

N.	Requisito	Adeguato/Non Adeguato - Note			
		SI	NO	Risk Level	
20	Ha il titolare aderito ad un codice di condotta o ad un sistema di certificazione?	X		1	
21	Il registro contiene l'informazione circa l'adesione del titolare al codice di condotta/sistema di certificazione?	X		1	
22	Esplicita il registro le misure tecniche ed organizzative implementate e riconducibili al codice di condotta e/o al sistema di certificazione	X		1	
23	Reca il registro la data della sua emissione?	X		1	
24	E' specificato se si tratta di prima emissione o di successiva revisione?	X		1	
25	E', il registro, sottoscritto dalla funzione che in base al sistema di procure e deleghe dell'organizzazione è deputata a farlo?	X		1	
26	E' stabilita la modalità di conservazione del registro?	X		1	
27	E' definito l'ambito di distribuzione interna del registro?	X		1	
28	E' individuata la funzione responsabile della conservazione e distribuzione interna del registro?	X		1	
29	Il titolare ha pianificato la revisione del registro?	X		1	
30	Altro				

7) - Analisi dei trattamenti di dati personali – Mappa dei trattamenti di dati personali

6.1 Trattamento finalizzato alla gestione del rapporto di lavoro		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Trattamento necessario per la gestione del rapporto di lavoro o di collaborazione. In questo trattamento rientrano anche la: • gestione della struttura organizzativa, dell'anagrafica del personale e registrazione degli eventi di carriera; • gestione delle pratiche assicurative e previdenziali; trattamenti assistenziali; denunce e pratiche di infortunio, trattamenti assistenziali; • trattamento dei dati inerenti i procedimenti disciplinari a carico del personale e nei giudizi pendenti di fronte a tutte le giurisdizioni che coinvolgono lavoratori e collaboratori; • gestione delle risorse umane (posizioni organizzative, profili di competenza, processo di selezione, politiche retributive); • gestione della formazione; • rilevazione e gestione delle presenze; • gestione retributiva; • gestione dei provvedimenti per il personale (es. mobilità, trasferimenti, ecc.); • programmazione annuale degli obiettivi e dei progetti, finalizzata alla valutazione del personale, alla pianificazione finanziaria e alla predisposizione del budget di Area/Amministrazione.	Adeguato
Natura dei dati	Personali, categorie particolari di dati personali.	Adeguato
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Il principio di minimizzazione impone una selezione dei dati da trattare in relazione allo specifico servizio o finalità perseguita, ad esempio: • per la gestione dei dati anagrafici e amministrativo contabili dei lavoratori e collaboratori esterni possono essere trattati dati inerenti l'anagrafica, dati bancari, fiscali e previdenziali; • per la gestione del lavoratore possono essere trattati dati relativi alla costituzione/cessazione del rapporto di lavoro, alle procedure di valutazione comparativa, al reclutamento, agli affidamenti, agli incarichi esterni; • per la gestione degli istituti contrattuali possono essere trattati dati relativi a congedi, permessi, aspettative, malattie, infortuni, partecipazioni a scioperi e assemblee, ecc.	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'assunzione e dell'avvio del rapporto di collaborazione.	Adeguato
Archiviazione e conservazione (tempi, modi, quali dati)	Rispetto ai tempi di archiviazione/conservazione si specifica quanto segue: • L'anagrafica e i dati di carriera sono conservati dall'Ente illimitatamente nel tempo; • I dati inerenti graduatorie o verbali sono conservati illimitatamente nel tempo; • La conservazione dei restanti dati è sotteso ai tempi di conservazione degli atti amministrativi che li contengono (es. 10 anni).	Adeguato
Categorie di interessati	Tutti i dipendenti dell'organizzazione e collaboratori	Adeguato

6.1 Trattamento finalizzato alla gestione del rapporto di lavoro		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Categorie di destinatari	Strutture dell'Ente (ad es. Uffici del Personale ecc.) Altri soggetti pubblici o privati, tra cui: • Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000; • INPS (per erogazione e liquidazione trattamento di pensione, L. 335/1995; L. 152/1968); • INAIL, Autorità di P.S., Sportello unico per l'immigrazione (DPR n. 334/2004) e/o altre Autorità previste dalla legge (per denuncia infortunio, DPR 1124/1965); • Strutture sanitarie competenti (per visite fiscali, art. 21 CCNL del 06/07/1995, CCNL di comparto); • Soggetti pubblici e privati ai quali, ai sensi delle leggi regionali/provinciali, viene affidato il servizio di formazione del personale; • Direzione Territoriale del lavoro (per le aspettative e per i casi di contenzioso); • Centro per l'impiego o organismo territorialmente competente per le assunzioni ai sensi della legge 68/1999; • Amministrazioni provinciali e Centro regionale per l'impiego in ordine al prospetto informativo delle assunzioni, cessazioni e modifiche al rapporto di lavoro, redatto ai sensi della L. 68/1999; • Autorità giudiziaria (C.P. e C.P.P.); • Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali; • Ministero delle Finanze, Centro di assistenza fiscale (CAF), relativamente alla dichiarazione dei redditi dei dipendenti (art.17 D.M. 164/1999 e art. 2-bis D.P.R. 600/1973); • Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, nell'ambito della mobilità dei lavoratori.	Adeguato
Comunicazione e trasferimento all'estero e/o su larga scala	I dati personali potrebbero essere trasferiti all'estero nel caso di periodi di formazione del personale all'estero.	Adeguato
Note sui diritti dell'interessato	In merito alla cancellazione dei dati – non può essere concessa la cancellazione di dati personali che, per la normativa vigente devono essere conservati illimitatamente nel tempo.	Adeguato

6.2 Trattamento finalizzato all'assunzione e alle attività di formazione-addestramento e aggiornamento professionale		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Il trattamento di dati personali è svolto per l'erogazione di attività didattiche e di formazione/aggiornamento (frontale, multimediale e a distanza). Rientrano in questo tipo di trattamento anche i trattamenti per: • Iscrizione a corsi di formazione; • Gestione dei registri delle attività didattiche: consuntivazione attività didattiche e non, a preventivo e consuntivo; • Valutazioni qualità, nell'ipotesi in cui i questionari possano essere indirettamente riconducibili a un interessato; • Eventuali attestati di frequenza ai corsi.	Adeguato
Natura dei dati	Personali, categorie particolari di dati personali (solo per i casi in cui debbano essere predisposte misure particolari per l'organizzazione dei corsi).	Adeguato
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	In relazione allo specifico corso/servizio erogato, potrebbero essere trattati: dati presenti in anagrafica, dati di carriera, curriculum vitae, ore di rendicontazione della docenza, iscrizioni e partecipazioni a corsi di formazione.	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	L'informativa potrebbe essere inclusa tra le informazioni rese al momento della gestione del rapporto di dipendenza o collaborazione. Nel caso in cui, durante la sessione di formazione, siano registrate le immagini e/o le voci di docenti e/o partecipanti, si rende opportuno informare gli interessati di tale trattamento mediante, ad esempio, affissione dei cartelli informativi.	Adeguato
Archiviazione e conservazione (tempi, modi, quali dati)	Gli atti connessi alle attività di formazione svolte dai partecipanti potrebbero avere un tempo di conservazione illimitato. La conservazione delle registrazioni audio/video dovrà essere stabilita nell'informativa in relazione alle specifiche finalità perseguite dall'ente.	Adeguato
Categorie di interessati	Lavoratori.	Adeguato

6.2 Trattamento finalizzato all'assunzione e alle attività di formazione-addestramento e aggiornamento professionale		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Categorie di destinatari	Strutture dell'Ente deputate alla formazione e all'aggiornamento professionale di dipendenti e collaboratori e/o altre Aziende (ad esempio nell'ambito di corsi di formazione erogati tra più università partner). Enti/Aziende esterne eroganti il servizio di formazione e aggiornamento professionale. Enti pubblici convenzionati, con lo scopo di migliorarne la fruibilità e di garantire la qualità e l'efficacia della formazione sul territorio nazionale.	Adeguato
Note sui diritti dell'interessato	Potrebbe essere garantita l'opposizione a specifiche operazioni di trattamento delle riprese audio-video (es. nel caso di diffusione del video su internet)	Adeguato
Comunicazione e trasferimento all'estero e/o su larga scala	-	Adeguato

6.3 Trattamento per la salute e la sicurezza delle persone nei luoghi di lavoro -Trattamenti effettuati dal Medico Competente		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Il dato è trattato dal Medico Competente al fine di svolgere l'attività di sorveglianza sanitaria obbligatoria del personale, ottemperando agli obblighi di legge come definiti dal D.Lgs.81/08 - Testo Unico in materia di salute e sicurezza del lavoro.	Adeguato
Natura dei dati	Personali, categorie particolari di dati personali (dati inerenti lo stato di salute, referti medici, ecc.)	Adeguato
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, dati di contatto, dati inerenti lo stato di salute, dati inerenti l'attività lavorativa svolta e di carriera.	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Informativa specifica per il servizio da rendere all'interessato all'atto dell'assunzione e/o della visita medica.	Adeguato
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi di conservazione dei dati sono strettamente dipendenti dagli ambiti di gestione (es: fascicolo sanitario/referti/gestione amministrativa), per tutta la durata del rapporto di lavoro e dalle norme vigenti in tali ambiti.	Adeguato
Categorie di interessati	Tutti i lavoratori dell'organizzazione sulla base dei protocolli di rischio in rapporto alle attività svolte.	Adeguato
Categorie di destinatari	Servizio Prevenzione di Prevenzione, Protezione e Sicurezza; Ufficio Personale, ecc.	Adeguato
Note sui diritti dell'interessato	-	Adeguato
Comunicazione e trasferimento all'estero e/o su larga scala	I dati non vengono comunicati all'estero, salvo casi specifici che lo richiedano (es. lavoratori distaccati presso stabilimenti e/o cantieri all'estero).	Adeguato

6.4 Trattamento per la salute e la sicurezza delle persone nei luoghi di lavoro -Trattamenti effettuati dal Servizio di Prevenzione Protezione e Sicurezza		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Il dato è trattato dal Servizio di Prevenzione, Protezione e Sicurezza al fine di supportare il Medico Competente nell'attività di sorveglianza sanitaria obbligatoria del personale, ottemperando agli obblighi di legge come definiti dal D.Lgs.81/08.	Adeguato
Natura dei dati	Personali, categorie particolari di dati personali (dati inerenti lo stato di salute).	Adeguato
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, dati di contatto, dati inerenti lo stato di salute, dati inerenti l'attività lavorativa svolta e di carriera.	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità sono inseriti nell'informativa generale resa al momento dell'assunzione.	Adeguato
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi di conservazione dei dati sono strettamente dipendenti dagli ambiti di gestione (es: fascicolo sanitario/referti/gestione amministrativa), per tutta la durata del rapporto di lavoro e dalle norme vigenti in tali ambiti.	Adeguato

6.4 Trattamento per la salute e la sicurezza delle persone nei luoghi di lavoro -Trattamenti effettuati dal Servizio di Prevenzione Protezione e Sicurezza		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Categorie di interessati	Tutti i lavoratori dell'organizzazione sulla base dei protocolli di rischio in rapporto alle attività svolte.	Adeguato
Categorie di destinatari	Ufficio Prevenzione, Protezione e Sicurezza; Ufficio Personale, Responsabili di struttura.	Adeguato
Note sui diritti dell'interessato	-	Adeguato
Comunicazione e trasferimento all'estero e/o su larga scala	I dati non vengono comunicati all'estero, salvo casi specifici che lo richiedano (es. lavoratori distaccati presso stabilimenti e/o cantieri all'estero).	Adeguato

6.5 Trattamento per la gestione degli infortuni		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Il trattamento viene effettuato in relazione agli infortuni occorsi ai lavoratori. In particolare nell'ambito della gestione di tali eventi da parte degli uffici preposti, dalla presa in carico della segnalazione di infortunio fino alla chiusura della relativa pratica, includendo: • l'interazione con enti esterni; • la gestione di eventuali prescrizioni da parte dell'INAIL; • l'apertura e gestione della segnalazione di sinistro nell'ambito di copertura delle polizze assicurative dell'Ente; • la valutazione delle proposte di liquidazione del danno; • gli eventuali prolungamenti del periodo di infortunio.	Adeguato
Natura dei dati	Personali, categorie particolari di dati personali (dati inerenti lo stato di salute).	Adeguato
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici e dati inerenti lo stato di salute. Dati specifici relativi all'infortunio occorso (es referti, certificati).	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti all'atto dell'apertura del sinistro.	Adeguato
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi di conservazione dei dati sono strettamente dipendenti dagli ambiti di gestione (es: fascicolo sanitario/referti/gestione amministrativa), per tutta la durata del rapporto di lavoro e dalle norme vigenti in tali ambiti.	Adeguato
Categorie di interessati	Tutti i lavoratori dell'organizzazione sulla base dei protocolli di rischio in rapporto alle attività svolte.	Adeguato
Categorie di destinatari	Uffici dell'Ente coinvolti nella gestione degli infortuni, broker, compagnia assicuratrice, INAIL, eventuali ulteriori enti coinvolti (Aziende ospedaliere).	Adeguato
Note sui diritti dell'interessato	-	Adeguato
Comunicazione e trasferimento all'estero e/o su larga scala	I dati non vengono comunicati all'estero, salvo casi specifici che lo richiedano (es. lavoratori distaccati presso stabilimenti e/o cantieri all'estero).	Adeguato

6.6 Trattamento di dati nell'ambito dei servizi di conservazione documentale - Trattamento finalizzato alla gestione del protocollo in entrata/uscita		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Gestione del protocollo informatico nelle fasi di entrata/uscita al fine di fornire data e ora certa agli atti acquisiti o trasmessi. Le registrazioni di protocollo ed i file a esso associati, prodotti e raccolti nell'ambito delle funzioni dell'Ente ed entro le Aree Organizzative Omogenee dello stesso per l'espletamento di procedimenti, affari ed attività, sono: • accessibili ai responsabili ed agli operatori preposti, con diritti di registrazione e consultazione definiti da specifiche policy indicate nel manuale di gestione del protocollo; • ottemperano quando previsto dal DPCM 3.13.2013 – regole tecniche per il protocollo informatico e in particolare dagli articoli 6, 7, 8, 18, 20, 21; • sottoposte alla gestione dei pacchetti di distribuzione e di versamento sulla base degli accordi presi con il conservatore accreditato prescelto.	Adeguato

6.6 Trattamento di dati nell'ambito dei servizi di conservazione documentale - Trattamento finalizzato alla gestione del protocollo in entrata/uscita		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Natura dei dati	In funzione del procedimento/attività i documenti possono contenere dati personali, anche appartenenti a particolari categorie (es particolari o giudiziari). Ogni dato e documento inserito nel sistema di protocollo potrebbe contenere tali dati nella: • descrizione del documento e sua rappresentazione, oggetto, allegati, classificazione, file associati (nativi digitali o loro conversione in formato digitale); • indicazione dei corrispondenti/contraenti e dei responsabili e assegnatari del documento.	Adeguato
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici dei mittenti e destinatari. Il campo oggetto, incluso nel nucleo minimo delle informazioni necessarie per la registrazione a protocollo, potrebbe per sua natura riportare dati personali, anche appartenenti a particolari categorie (es particolari o giudiziari). I dati trattati dipendono dallo specifico procedimento/attività e sempre nell'osservanza del DPCM 3.12.2013, tanto in materia di protocollo informatico (ai sensi degli articoli 40bis, 41, 47, 57bis e 71 del CAD) tanto in materia di conservazione (ai sensi degli articoli 20, commi 3 e 5bis, 23ter, comma 3, 43, commi 1 e 3, 44, 44bis e 71 comma 1 del CAD). Potrebbe rendersi necessaria anche la registrazione di ulteriori dati personali per supportare e motivare (a titolo di esempio): • la creazione del pacchetto di distribuzione per motivi legali o accessi agli atti concorsuali; • l'accesso al sistema di conservazione per la verifica dell'operato del conservatore o per verifiche di carattere tecnico.	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa: • al momento dell'assunzione, per il Lavoratore; • all'inizio di un rapporto di collaborazione con un soggetto esterno.	Adeguato
Archiviazione e conservazione (tempi, modi, quali dati)	Il tempo di conservazione dei dati dipende dallo specifico procedimento/attività e si basa su quanto previsto da obblighi di legge e regolamenti interni.	Adeguato
Categorie di interessati	Tutti i lavoratori dell'organizzazione e soggetti esterni.	Adeguato
Categorie di destinatari	Strutture dell'Ente e loro operatori e delegati preposti al processo di gestione documentale attraverso l'utilizzo dei sistemi di protocollo informatico o applicativi verticali che concorrono al popolamento del registro di protocollo informatico. Mittenti o destinatari delle registrazioni a protocollo.	Adeguato
Note sui diritti dell'interessato	-	Adeguato
Comunicazione e trasferimento all'estero e/o su larga scala	-	Adeguato

6.7 Trattamento finalizzato alla conservazione documentale		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Gestione delle attività di conservazione documentale ai sensi della normativa vigente	Adeguato
Natura dei dati	Ogni dato e documento inserito nel sistema di protocollo informatico e potenziale oggetto di invio in conservazione, ovvero: • descrizione del documento e sua rappresentazione, ovvero numero di protocollo ed eventuale repertorio, data, oggetto, allegati, classificazione, file associati (nativi digitali o loro conversione in formato digitale); • indicazione dei corrispondenti/contraenti e dei responsabili e assegnatari del documento; • In funzione del procedimento/attività i documenti possono contenere dati personali, anche appartenenti a particolari categorie (es. particolari o giudiziari).	Adeguato

6.7 Trattamento finalizzato alla conservazione documentale		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici dei mittenti e destinatari. Il campo oggetto, incluso nel nucleo minimo delle informazioni necessarie per la registrazione a protocollo, potrebbe per sua natura riportare dati personali, anche appartenenti a particolari categorie (es particolari o giudiziari). I dati trattati dipendono dallo specifico procedimento/attività e sempre nell'osservanza del DPCM 3.12.2013, tanto in materia di protocollo informatico (ai sensi degli articoli 40bis, 41, 47, 57bis e 71 del CAD) tanto in materia di conservazione (ai sensi degli articoli 20, commi 3 e 5bis, 23ter, comma 3, 43, commi 1 e 3, 44, 44bis e 71 comma 1 del CAD). Potrebbe rendersi necessaria anche la registrazione di ulteriori dati personali per supportare e motivare (a titolo di esempio): • la creazione del pacchetto di distribuzione per motivi legali o accessi agli atti concorsuali; • l'accesso al sistema di conservazione per la verifica dell'operato del conservatore o per verifiche di carattere tecnico.	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa: • al momento dell'assunzione, per il Lavoratore; • all'inizio di un rapporto di collaborazione con un soggetto esterno.	Adeguato
Archiviazione e conservazione (tempi, modi, quali dati)	Il tempo di conservazione dei dati dipende dallo specifico procedimento/attività e si basa su quanto previsto da obblighi di legge e regolamenti interni.	Adeguato
Categorie di interessati	Tutti i lavoratori dell'organizzazione e soggetti esterni.	Adeguato
Categorie di destinatari	Strutture dell'Ente e loro operatori e delegati preposti al processo di gestione documentale attraverso l'utilizzo dei sistemi di protocollo informatico o applicativi verticali che concorrono al popolamento del registro di protocollo informatico. Mittenti o destinatari delle registrazioni a protocollo.	Adeguato
Note sui diritti dell'interessato	-	Adeguato
Comunicazione e trasferimento all'estero e/o su larga scala	-	Adeguato

6.8 Trattamento finalizzato all'acquisizione di beni e servizi		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Il dato è trattato per consentire la verifica di posizioni giudiziarie, fiscali e di condotta di fornitori ed operatori economici che sono in rapporto con l'Ente al fine di: • svolgere le attività preliminari connesse alle procedure di acquisizione di beni e servizi; • coordinare e analizzare la redazione della documentazione tecnica, amministrativa e contrattuale; • gestire il procedimento e le attività connesse (stipula del contratto, monitoraggio dei tempi del procedimento in affidamento, ecc.).	Adeguato
Natura dei dati	Personali, dati personali relativi a condanne penali e reati	Adeguato
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Potrebbe rendersi necessaria la registrazione di dati personali presenti nella documentazione inerente: • DURC (acquisendo parte dei dati da Inps e altri da INAIL); • Visure camerali (acquisiti da Infocamere); • Certificato di Casellario Giudiziale (Tribunale); • accertamenti sulla situazione societaria e personale delle controparti; • verifica regolarità fiscale (Agenzia delle entrate ed Equitalia per il pregresso). Nel caso di acquisti sopra soglia è necessario altresì acquisire i dati inerenti: • Offerta economica, in sede di verifica dell'offerta; • certificazioni antimafia (acquisita presso la Prefettura/Questura).	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	L'informativa può essere resa al momento richiesta dell'offerta per la fornitura di beni o servizi. Al momento della stipula del contratto e/o conferma dell'ordine di acquisto si può consegnare un'ulteriore informativa più specifica in funzione del servizio reso o del bene acquisito.	Adeguato

6.8 Trattamento finalizzato all'acquisizione di beni e servizi		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi possono essere molto diversi a seconda del tipo di contratto e dell'oggetto della fornitura. Il criterio per stabilirli si basa su principi di buon senso e sulle precisazioni dell'Autorità Garante secondo cui i dati possono essere conservati in generale "finché sussista un interesse giustificabile" e cioè finché la loro conservazione risulti necessaria agli scopi per i quali sono stati raccolti e trattati. Ad esempio nel caso in cui si acquisti un bene con garanzia a vita o un software con licenza d'uso illimitata in senso temporale i dati possono essere conservati a tempo indeterminato, comunque fino a che il bene o il software non viene dismesso. Più in generale, i dati dovrebbero essere conservati in linea con quanto previsto dal Codice Civile (art. 2220).	Adeguato
Categorie di interessati	Fornitori di beni e servizi, operatori economici.	Adeguato
Categorie di destinatari	Strutture preposte all'acquisto di beni e servizi, alla liquidazione e alla gestione del pagamento o alla gestione del contenzioso; struttura preposta al rispetto delle norme su trasparenza e anticorruzione.	Adeguato
Note sui diritti dell'interessato	-	Adeguato
Comunicazione e trasferimento all'estero e/o su larga scala	-	Adeguato

6.9 Trattamento finalizzato alle verifiche sull'espletamento di lavori, in cantiere o presso terzi		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Il dato è trattato per la valutazione amministrativa ed economica di terzi, fornitori dell'Ente per l'espletamento di lavori in appalto, verifiche sui cantieri o presso attività in esterno.	Adeguato
Natura dei dati	Personali, categorie particolari di dati personali, dati personali relativi a condanne penali e reati.	Adeguato
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Potrebbe rendersi necessaria la registrazione di dati personali per consentire, ad esempio: • La consultazione del contratto dei lavoratori delle ditte appaltatrici e di quelle sub-appaltate; • La verifica di atti relativi ai dipendenti delle società.	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	L'informativa può essere resa al momento richiesta dell'offerta per la fornitura di beni o servizi. Al momento della stipula del contratto e/o conferma dell'ordine di lavoro si può consegnare un'ulteriore informativa più specifica in funzione del servizio reso o del bene.	Adeguato
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi di conservazione dei dati dipendono dallo specifico procedimento e dalla normativa vigente in materia di appalti, sicurezza sul lavoro e conduzione di cantieri.	Adeguato
Categorie di interessati	Fornitori di beni e servizi, operatori economici.	Adeguato
Categorie di destinatari	Strutture preposte alla vendita di beni e servizi, alla gestione dell'incasso o alla gestione del contenzioso; struttura preposta al rispetto delle norme su trasparenza e anticorruzione.	Adeguato
Note sui diritti dell'interessato	-	Adeguato
Comunicazione e trasferimento all'estero e/o su larga scala	-	Adeguato

6.10 Trattamento finalizzato alla gestione del contenzioso e del recupero crediti		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Il dato è trattato per: • la gestione dei contenziosi instaurati avanti le diverse autorità giudiziarie in cui sia coinvolto l'Ente; • l'attività di recupero dei crediti dell'Ente nei confronti di soggetti terzi inadempienti.	Adeguato
Natura dei dati	Personali, categorie particolari di dati personali, dati personali relativi a condanne penali e reati.	Adeguato

6.10 Trattamento finalizzato alla gestione del contenzioso e del recupero crediti		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	I dati trattati possono essere differenti a seconda del tipo di contenzioso; includerà in ogni caso i dati anagrafici e il tipo di rapporto con l'Ente; potrebbe includere dati sanitari. Per il recupero crediti, la tipologia di dati trattati sarà in correlazione alla categoria di interessati coinvolta.	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità potrebbero essere inserite in un'apposita informativa o nell'informativa generale resa: • al personale dipendente; • ai lavoratori; • a soggetti terzi e aziende fornitrici di beni e servizi.	Adeguato
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi di conservazione sono definiti dalla legge.	Adeguato
Categorie di interessati	Sono interessati potenzialmente tutti i soggetti che abbiano un rapporto con l'Ente: personale dipendente, lavoratori, operatori economici, soggetti terzi (fornitori). Può interessare anche persone che non hanno rapporti di alcun tipo con l'Ente (es. persona che accede ai locali per informazioni). Con riguardo ad alcuni contenziosi e procedimenti di recupero crediti potrebbero essere interessati anche i familiari dei soggetti direttamente coinvolti.	Adeguato
Categorie di destinatari	Ufficio d'Ente preposto, Autorità Giudiziarie e Agenzia delle Entrate (nel caso di iscrizione a ruolo dei crediti). Strutture preposte alla vendita di beni e servizi, alla gestione dell'incasso o alla gestione del contenzioso; struttura preposta al rispetto delle norme su trasparenza e anticorruzione.	Adeguato
Note sui diritti dell'interessato	-	Adeguato
Comunicazione e trasferimento all'estero e/o su larga scala	Potrebbe esser necessaria la comunicazione e/o il trasferimento di dati all'estero nei casi di contenzioso con soggetti esteri e nel caso di recupero crediti da debitori esteri, con affidamento della pratica a professionisti stabiliti nei paesi dei soggetti con i quali si sia instaurata la lite.	Adeguato

6.11 Trattamento di dati nell'ambito dei servizi elettronici e strumenti di collaboration		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Al fine di favorire il business e lo sviluppo economico, l'Ente potrebbe fornire strumenti informatici (es: web conference, spazi virtuali di collaborazione, ecc.) tramite i quali possono essere trattati dati personali funzionali: • all'erogazione del servizio stesso; • alla valutazione dell'uso del servizio e della qualità (es: mediante rilevazioni statistiche basate sull'uso di tali strumenti); • a garantire la sicurezza informativa dei dati trattati mediante tali strumenti di collaboration.	Adeguato
Natura dei dati	Personali, categorie particolari di dati personali.	Adeguato
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	A seconda del tipo di attività o strumento di collaborazione potrebbero essere utilizzati dati quali, l'indirizzo di posta elettronica, l'indirizzo IP del sistema utilizzato, dati relativi alla carriera, dati anagrafici, ecc.	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	L'informativa dovrebbe essere resa prima dell'accesso al sistema, qualora non specificato in informative specifiche.	Adeguato
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi possono essere molto diversi a seconda del tipo di strumento utilizzato e della finalità perseguita. Il criterio per stabilirli si basa su principi di buon senso e sulle precisazioni dell'Autorità Garante secondo cui i dati possono essere conservati in generale "finché sussista un interesse giustificabile" e cioè finché la loro conservazione risulti necessaria agli scopi per i quali sono stati raccolti e trattati. Normalmente tale periodo di conservazione non supera i 6 mesi.	Adeguato
Categorie di interessati	Personale dipendente, collaboratori esterni, lavoratori, altri soggetti utilizzatori del servizio.	Adeguato
Categorie di destinatari	Uffici dell'Ente preposto alla gestione e/o utilizzo dello strumento di collaboration.	Adeguato
Note sui diritti dell'interessato	-	Adeguato
Comunicazione e trasferimento all'estero e/o su larga scala	Solo in caso di servizio erogato outsourcer estero e nel caso in cui sia lecita la comunicazione di tali dati personali.	Adeguato

6.12 Trattamento di dati nell'ambito dei servizi di posta elettronica		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Al fine di favorire la comunicazione tramite i servizi di posta elettronica, l'Ente potrebbe trattare dati personali funzionali a: • l'erogazione del servizio stesso; • lo svolgimento attività connesse alla risoluzione dei guasti (troubleshooting); • la valutazione dell'uso del servizio e della qualità dei servizio (es: mediante rilevazioni statistiche basate sull'uso di tali strumenti); • garantire la sicurezza informativa dei dati trattati (tramite ad esempio la gestione di incidenti di sicurezza e tramite azioni preventive sulla diffusione di messaggi contenenti malware).	Adeguato
Natura dei dati	Personali, categorie particolari di dati personali.	Adeguato
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Indirizzi e-mail. All'atto della creazione dell'account o in caso di cambio di status (se sono previste differenze di gestione delle caselle a seconda del ruolo), anche anagrafica dell'utente (codice fiscale, ruolo ricoperto, mansione, ecc.). Nella gestione legata al troubleshooting, incidenti di sicurezza e azioni preventive sulla diffusione di messaggi malevoli, potrebbe rendersi necessario il trattamento dei seguenti dati connessi ai messaggi di posta: casella di posta sorgente, casella destinataria, server in entrata e uscita, server di transito, oggetto mail, timestamp.	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa: • all'assunzione, per il personale dipendente; • alla richiesta di creazione dell'account per soggetti terzi.	Adeguato
Archiviazione e conservazione (tempi, modi, quali dati)	In generale dipende dai regolamenti interni, che spesso prevedono differenze di trattamento a seconda del tipo di utente (es. tempi di cancellazione della casella di posta diversi a seconda del ruolo).	Adeguato
Categorie di interessati	Personale dipendente, collaboratori esterni, lavoratori, altri soggetti utilizzatori del servizio.	Adeguato
Categorie di destinatari	Uffici dell'Ente preposto alla gestione e/o utilizzo dello strumento di collaboration.	Adeguato
Note sui diritti dell'interessato	Cancellazione solo dopo un determinato periodo dalla cessazione del rapporto.	Adeguato
Comunicazione e trasferimento all'estero e/o su larga scala	Solo in caso di servizio erogato outsourcer estero e nel caso in cui sia lecita la comunicazione di tali dati personali.	Adeguato

6.13 Trattamento finalizzato ad attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Il dato potrebbe essere trattato: • per finalità di reperimento fondi; • sviluppo di community relativi a lavoratori dell'Ente; • promozione dell'immagine dell'Ente e delle sue attività, conferendo conoscenza e visibilità ad eventi organizzati dallo stesso e nei quali è coinvolto.	Adeguato
Natura dei dati	Personali.	Adeguato
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, di contatto, eventuali video e immagini di lavoratori, soggetti terzi, ecc.	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Si precisa che il trattamento dei dati svolto nell'ambito delle diverse finalità potrebbe essere differente e richiedere specifiche informative.	Adeguato
Archiviazione e conservazione (tempi, modi, quali dati)	Nessun vincolo di conservazione, archiviazione di lungo periodo a fronte del consenso dell'interessato.	Adeguato
Note sui diritti dell'interessato	-	Adeguato
Categorie di interessati	Lavoratori e Terzi.	Adeguato
Categorie di destinatari	Strutture dell'Ente preposte al servizio, servizi esterni di gestione community e/o fundraising, società organizzatrici di eventi, ecc.	Adeguato

6.14 Trattamento finalizzato ad attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Il dato potrebbe essere trattato: • per finalità di reperimento fondi; • sviluppo di community relativi a lavoratori dell'Ente; • promozione dell'immagine dell'Ente e delle sue attività, conferendo conoscenza e visibilità ad eventi organizzati dallo stesso e nei quali è coinvolto.	Adeguato
Natura dei dati	Personali.	Adeguato
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, di contatto, eventuali video e immagini di lavoratori, soggetti terzi, ecc.	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Si precisa che il trattamento dei dati svolto nell'ambito delle diverse finalità potrebbe essere differente e richiedere specifiche informative.	Adeguato
Archiviazione e conservazione (tempi, modi, quali dati)	Nessun vincolo di conservazione, archiviazione di lungo periodo a fronte del consenso dell'interessato.	Adeguato
Note sui diritti dell'interessato	-	Adeguato
Categorie di interessati	Lavoratori e Terzi.	Adeguato
Categorie di destinatari	Strutture dell'Ente preposte al servizio, servizi esterni di gestione community e/o fundraising, società organizzatrici di eventi, ecc.	Adeguato
Comunicazione e trasferimento all'estero e/o su larga scala	Sono nel caso in cui i destinatari sopra riportati operino/trattino i dati in aree extra UE.	Adeguato

6.15 Trattamento finalizzato a rilevazioni statistiche		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Il dato è trattato a fini di rilevazioni statistiche volte a perseguire fini istituzionali dell'Ente (es: attività di ricerca o attività di quality assurance o attività volte a migliorare l'immagine complessiva).	Adeguato
Natura dei dati	Personali.	Adeguato
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dipende dalla rilevazione richiesta e dall'ambito. Esempio: potrebbero essere trattati dati anagrafici (e/o di contatto) e dati di carriera per verificare l'adeguatezza della formazione acquisita in università, la coerenza delle competenze apprese rispetto alla futura attività lavorativa dello studente, l'utilità del titolo ottenuto rispetto all'attività lavorativa svolta o da svolgere.	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	L'informativa dovrà dettagliare le specifiche finalità della rilevazione tenuto comunque conto di quanto riferito nella legge.	Adeguato
Archiviazione e conservazione (tempi, modi, quali dati)	Nessun vincolo di conservazione. Conservazione dei dati dipende dal tempo definito per la finalità della raccolta posta in origine.	Adeguato
Note sui diritti dell'interessato	Cancellazione non possibile per questionari anonimizzati.	Adeguato
Categorie di interessati	Lavoratori.	Adeguato
Categorie di destinatari	Tutto il personale dell'organizzazione e soggetti terzi.	Adeguato

6.16 Procedimenti di natura disciplinare a carico di lavoratori		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Il trattamento è finalizzato allo svolgimento di procedimenti disciplinari a carico di lavoratori	Adeguato
Natura dei dati	Personali, categorie particolari di dati personali e dati personali relativi a condanne penali e reati.	Adeguato
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, di carriera e dati inerenti lo specifico procedimento.	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'assunzione.	Adeguato
Archiviazione e conservazione (tempi, modi, quali dati)	Basato su obblighi di legge e regolamenti. Il periodo di conservazione indicato in alcuni massimari di scarto per la conservazione degli atti connessi a questa attività è: - illimitato, per il provvedimento disciplinare; - 5 anni per i provvedimenti revocati o annullati.	Adeguato
Note sui diritti dell'interessato	-	Adeguato
Categorie di interessati	Lavoratori, autorità giudiziaria.	Adeguato
Categorie di destinatari	Lavoratori e personale dell'organizzazione.	Adeguato

6.17 Trattamento per la gestione degli infortuni		
Elementi considerati		**Note: Adeguato/Non Adeguato**
Descrizione del trattamento	Il trattamento viene effettuato in relazione agli infortuni occorsi ai lavoratori. In particolare nell'ambito della gestione di tali eventi da parte degli uffici preposti, dalla presa in carico della segnalazione di infortunio fino alla chiusura della relativa pratica, includendo: - l'interazione con enti esterni - la gestione di eventuali prescrizioni da parte dell'INAIL - l'apertura e gestione della segnalazione di sinistro nell'ambito di copertura delle polizze assicurative - la valutazione delle proposte di liquidazione del danno - gli eventuali prolungamenti del periodo di infortunio.	Adeguato
Natura dei dati	Personali, categorie particolari di dati personali (dati inerenti lo stato di salute).	Adeguato
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, di carriera e dati inerenti lo stato di salute. Dati specifici relativi all'infortunio occorso (es referti, certificati).	Adeguato
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti all'atto dell'apertura del sinistro.	Adeguato
Archiviazione e conservazione (tempi, modi, quali dati)	Il tempo di conservazione dei dati dipende dallo specifico procedimento e si basa su quanto previsto da obblighi di legge o regolamenti interni.	Adeguato
Categorie di interessati	Lavoratore infortunato	Adeguato
Categorie di destinatari	Tutto il personale dell'organizzazione e soggetti terzi.	Adeguato
Comunicazione e trasferimento all'estero	Uffici coinvolti nella gestione degli infortuni, broker, compagnia assicuratrice, INAIL, eventuali ulteriori enti coinvolti (Aziende ospedaliere).	Adeguato
Note sui diritti dell'interessato	I dati saranno comunicati e/o trasferiti all'estero in presenza di una compagnia assicuratrice estera o nel caso di soggetti coinvolti in infortuni all'estero.	Adeguato

8) - Analisi sintetica dei rischi che incombono sui dati

Ad un livello generale sono state individuate le seguenti principali minacce alla sicurezza dei dati gestiti dall'ente, suddivise in tre macro categorie:

Calamità naturali	Minacce internazionali	Minacce involontarie
Terremoto Incendio Fulmine Inondazione	Accessi non autorizzati Virus informatici Furto di dati e di attrezzature hardware	Black out elettrico Malfunzionamenti nel software Malfunzionamenti nell'hardware Errori umani e/o imperizia nell'utilizzo del sistema informatico

In riferimento alla sicurezza dei dati personali gestiti dall'ente si pone i seguenti obbiettivi:

Obiettivo	Cosa significa
Riservatezza	I dati devono essere accessibili solo alle persone autorizzate
Integrità	I dati devono essere protetti da modificazioni e danneggiamenti
Disponibilità	I dati devono essere accessibili alle persone autorizzate

Attraverso l'implementazione di una serie di misure di sicurezza, esposte in dettaglio nei successivi paragrafi, si vuole ridurre le vulnerabilità del sistema informativo, raggiungendo un livello di rischio valutato accettabile. In sintesi:

Obiettivo	Cosa significa
Riservatezza	Ridurre il rischio che persone non autorizzate possano accedere alle informazioni
Integrità	Ridurre il rischio che le informazioni siano volutamente modificate o cancellate
Disponibilità	Ridurre il rischio di non poter accedere anche se autorizzati alle informazioni

9) – Privacy Policy

Raccolta dati per interesse legittimo e prevalente del Titolare

Il legittimo interesse del Titolare del trattamento dell'ente per il perseguimento delle proprie finalità, costituisce la base giuridica per la raccolta e il trattamento dei dati personali e sarà sempre bilanciato con i diritti dell'interessato. Il rapporto instaurato è di natura commerciale privatistica, e il termine massimo per la conservazione di tali dati sarà di dieci anni nel rispetto delle normative fiscali.
Per le altre finalità (es. messaggi commerciali, attività promozionali, ecc.) l'interessato ha sempre la possibilità di revocare il consenso al trattamento e chiedere la cancellazione dei propri dati personali.

Sito Web

In questa pagina si descrivono le modalità e le logiche del trattamento dei dati personali degli utenti (di seguito, anche gli utenti) che consultano il sito: www.felcaro.it.

L'informativa è resa ai sensi dell'art.13 del Regolamento europeo 2016/679 – Regolamento generale sulla protezione dei dati in materia di protezione dei dati personali a tutti gli utenti che, interagendo con il Sito, forniscono all'ente Felcaro S.a.s. di Felcaro Mauro & C. i propri dati personali.
La validità dell'informativa contenuta nella presente pagina è limitata al solo Sito e non si estende ad altri siti web eventualmente consultabili mediante collegamento ipertestuale.
Il titolare del trattamento dei dati raccolti è: Felcaro S.a.s. di Felcaro Mauro & C.

I trattamenti di dati connessi al modulo di richiesta informazioni hanno luogo presso la sede dell'ente e sono curati, tramite strumenti elettronici e previa adozione delle idonee misure di sicurezza, da personale in servizio presso l'ufficio incaricato del trattamento.
Tipologia dei dati e finalità del trattamento
Tutti i dati personali forniti attraverso il Sito saranno trattati in modo lecito e secondo correttezza al fine di fornire i servizi richiesti nonché di rispondere alle comunicazioni e alle domande degli utenti, sempre nel perseguimento degli scopi istituzionali dell'ente così come previsti dalla Legge.
Dati forniti volontariamente:
Attraverso il Sito è possibile inviare richieste e comunicazioni all'ente attraverso gli indirizzi di contatto riportati sul sito. Il conferimento di tali dati è obbligatorio, necessario per rispondere alle richieste inviate nonché per ricontattare il mittente per ottenere precisazioni in ordine a quanto segnalato.
Dati di navigazione:
In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) e altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente. I dati di navigazione vengono acquisiti non per finalità di identificazione degli utenti, ma all'unico fine di raccogliere, in forma anonima, informazioni statistiche sull'utilizzo del sito e dei suoi servizi.
Cookies
I cookies sono piccoli file di testo che i siti visitati inviano al terminale dell'utente, dove vengono memorizzati, per poi essere ritrasmessi agli stessi siti alla visita successiva.
Il Sito utilizza:

- cookie di sessione il cui utilizzo non è strumentale alla raccolta di dati personali identificativi dell'utente, essendo limitato alla sola trasmissione di dati identificativi di sessione nella forma di numeri generati automaticamente dal server. I cookie di sessione non sono memorizzati in modo persistente sul dispositivo dell'utente e vengono cancellati automaticamente alla chiusura del browser.
- cookie di terza parte per la visualizzazione dei video su YouTube. L'ente non ha accesso ai dati che sono raccolti e trattati in piena autonomia dalle terze parti. Per maggiori informazioni sulle logiche e le modalità di trattamento dei dati raccolti dai social network, gli utenti sono invitati a leggere le note informative sulla privacy fornite dai soggetti che forniscono i servizi in questione: YouTube https://www.google.it/intl/it/policies/privacy/cookies analytics utilizzati per raccogliere informazioni, in forma aggregata, sul numero degli utenti e su come gli stessi visitano il Sito.

L'ente si avvale del servizio Google Analytics, la cui cookie policy può essere visionata all'indirizzo https://support.google.com/analytics/answer/6004245. Al fine di rispettare la privacy dei nostri utenti, il servizio è utilizzato con la modalità "_anonymizeip" che consente di mascherare gli indirizzi IP degli utenti che navigano sul sito internet (maggiori informazioni sulla funzionalità). I dati sono raccolti all'unico fine di elaborare informazioni statistiche anonime sull'uso del Sito e per verificare il corretto funzionamento dello stesso; i dati di navigazione potrebbero essere utilizzati in vista dell'identificazione dell'utente solo nel caso in cui ciò fosse necessario per l'accertamento di reati di natura informatica.

I cookies tecnici non sono utilizzati per attività di profilazione dell'Utente.
L'Utente può scegliere di abilitare o disabilitare i cookies intervenendo sulle impostazioni del proprio browser di navigazione secondo le istruzioni rese disponibili dai relativi fornitori ai link di seguito indicati da: Chrome; Firefox; Safari; Internet Explorer, ecc.
Diritti degli interessati
Gli Utenti possono esercitare in qualsiasi momento i diritti previsti dall'art.7 del Regolamento europeo 2016/679 - Privacy, al fine di ottenere la conferma dell'esistenza o meno dei loro dati personali e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento, oppure la rettificazione. Ai sensi della medesima disposizione l'Utente potrà inoltre chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché opporsi in ogni caso, per motivi legittimi, al loro trattamento.
Le richieste vanno inviate all'indirizzo info@felcaro.it
Attraverso i medesimi recapiti, l'Utente potrà chiedere inoltre la lista aggiornata di tutti i Responsabili del trattamento nominati dal Titolare.
La Privacy Policy di questo ente pubblicata sul sito internet è soggetta ad aggiornamenti; gli Utenti sono pertanto invitati a verificarne periodicamente il contenuto.

Parte II – MISURE DI SICUREZZA ADOTTATE E DA ADOTTARE

10) - Misure per garantire l'integrità e la disponibilità dei dati

a) Trattamento con strumenti elettronici

Ogni utilizzo del sistema informativo della società diverso da finalità strettamente professionali è espressamente vietato.
Di seguito vengono esposte regole minime comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine della società stessa.
La società s'impegna a formare gli incaricati in merito ai rischi, alle procedure operative, alla prevenzione dei danni e, più in generale, alle problematiche relative alla sicurezza in materia di trattamento dei dati.

Utilizzo dell'elaboratore e della rete interna
L'accesso all'elaboratore della propria postazione di lavoro, sia esso collegato in rete o "stand alone", è protetto da un sistema di autenticazione.
La password assegnata non deve essere divulgata e deve essere custodita dall'assegnatario con la massima diligenza.
E' vietato installare qualsiasi software anche demo, senza autorizzazione.
Su ogni elaboratore dell'ente è stato installato un software antivirus per prevenire eventuali danneggiamenti all'hardware o al software causati dalla presenza o dall'azione di programmi virus informatici.
E' importante utilizzare questi software antivirus per controllare qualsiasi file di provenienza esterna all'ente.
Si ricorda che nonostante la presenza del software antivirus è possibile che riescano ugualmente ad installarsi nei computer virus informatici non identificati o riconoscibili.
Pertanto in caso si evidenzino anomalie di funzionamento del computer è importante darne rapida segnalazione al Responsabile del Trattamento/Titolare del Trattamento.
Le unità di rete e le aree di condivisione contengono informazioni strettamente professionali e non possono essere utilizzate per scopi diversi. Non bisogna dislocare stampanti e fax in aree accessibili a soggetti non abilitati al trattamento e non presidiate (ad esempio i corridoi degli uffici).

Utilizzo servizi vari su internet
I servizi on line devono essere esclusivamente finalizzati al reperimento di informazioni utili alla società.
Ogni altra utilizzazione dell'accesso su internet, non finalizzata al reperimento di informazioni utili all'ente, non pertinente all'attività lavorativa o di tipo personale non è consentita.
Al fine di non compromettere la sicurezza della società e di prevenire conseguenze legali o di altro genere, gli utenti dovranno adottare i seguenti comportamenti:

- evitare lo scaricamento di programmi software, anche gratuiti, se non per esigenze strettamente professionali e fatti comunque salvi i casi di esplicita autorizzazione;
- è vietata la partecipazione a Forum non professionali, l'utilizzo di chat, di bacheche elettroniche e, più in generale, qualunque utilizzo di servizi Internet, attuali o futuri, non strettamente inerenti all'attività professionale.

Utilizzo del servizio di posta elettronica
Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità dell'ente ed in stretta connessione con l'effettiva attività e mansioni del soggetto dipendente o collaboratore che utilizza tale funzionalità. Non è possibile utilizzare tale servizio per finalità in contrasto con quelle della società, o non pertinenti all'attività lavorativa o personali.
Al fine di non compromettere la sicurezza dell'ente e di prevenire conseguenze legali a carico della società stessa bisogna adottare le seguenti norme comportamentali:

- se nonostante i controlli preventivi antispamming e antivirus automatici, si ricevono mail da destinatari sconosciuti contenenti file (in particolare programmi eseguibili o file di word processor e fogli di calcolo contenenti delle macro, file compressi) evitare di aprire tali mail e tali file e procedere alla loro immediata eliminazione. Il comportamento sopradescritto va seguito anche se si ricevono file non concordati da destinatari conosciuti;
- è fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list salvo diversa ed esplicita autorizzazione;
- la casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.

Sistema di identificazione e autenticazione

L'ente ha attivato ed è correntemente funzionante un sistema d'autenticazione per ognuno degli incaricati che trattano dati personali.
E' stato attribuito un codice identificativo (username, user ID) collegato strettamente personale per l'utilizzazione degli strumenti elettronici (di solito personal computer) del sistema informatico.
Ad ogni incaricato possono eventualmente essere assegnati più codici per l'identificazione, ad esempio per funzioni diverse.
I codici identificativi sono frequentemente aggiornati, inserendo quelli dei nuovi incaricati e cancellando quelli degli incaricati non più autorizzati.
Il sistema di autenticazione prevede l'utilizzo di parole chiave (password) sia a livello di sistema operativo sia a livello di singola applicazione.
Le password da utilizzare devono:

- essere diverse da parole presenti nei vocabolari;
- non fare riferimento con informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro familiari;
- contenere una combinazione di numeri e lettere, maiuscole e minuscole.

Il Titolare del Trattamento è incaricato della gestione delle password dell'ente.
Non bisogna:

- rivelare la password a nessuno, soprattutto attraverso il telefono;
- scrivere la password in un messaggio di posta elettronica, o su supporti cartacei conservati in ufficio;
- rivelare o condividere la password con i colleghi di lavoro, famigliari e amici;
- utilizzare la caratteristica, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni;
- archiviare la password su un qualsiasi strumento elettronico, incluso il telefono cellulare, o su supporti cartacei conservati in ufficio, senza utilizzare un sistema di crittografia.

Viene segnalato agli incaricati che la lunghezza della password da utilizzare non deve essere inferiore ad otto caratteri, salvo limitazioni tecniche nei software in uso.
Si sollecita l'incaricato che riceve una password a modificarla al primo utilizzo.
L'incaricato deve segnalare al Titolare del Trattamento la sua password in uso che l'annota su un registro cartaceo conservato nella cassetta di sicurezza della banca e/o altro luogo adeguato.
Inoltre il sostituto dell'Incaricato al Trattamento dei dati deve essere messo in grado di poter lavorare sulla postazione di colui che sta sostituendo comunicandogli la password e l'id, in seguito a tale comunicazione è pertanto obbligato a rispettare il regolamento suddetto per quanto riguarda la selezione e gestione della password.
Viene segnalato ad ogni incaricato la necessità di cambiare la password almeno ogni 6 mesi.
Nell'ipotesi di trattamento di dati particolari viene segnalato ad ogni incaricato la necessità di cambiare password almeno ogni 3 mesi.
E' prevista una scadenza nella validità di ogni password utilizzata.
Sono vietate credenziali di autenticazione (username e password) condivise fra più persone.
Le credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate.
Le credenziali di autenticazione vengono immediatamente revocate in caso di provvedimenti disciplinari o quando si presentano situazioni che possono compromettere la sicurezza.
Sono state consegnate istruzioni scritte agli incaricati in merito alle modalità di gestione e di custodia delle password.
La visualizzazione della password sullo schermo dei personal computer è impedita da tutti i software in uso.
Il sistema di identificazione ed autenticazione è operativo anche sui computer portatili e sui palmari che possono gestire e contenere dati personali.

Adempimenti previsti per l'Amministratore di Sistema (Titolare Trattamento Dati)

Nel caso specifico il Titolare Trattamento Dati svolge funzioni di unico Amministratore di Sistema.
L'attribuzione di tale incarico è avvenuta previa valutazione delle sue caratteristiche di esperienza, capacità ed affidabilità e garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
Il controllo per la registrazione degli accessi ai sistemi di elaborazione ed agli archivi elettronici dell'Amministratore di Sistema avviene sulle proprie credenziali di accesso, non ritenendosi necessaria la registrazione dei file di log.
In questo caso non si applicano le previsioni relative alla verifica annuale delle attività di Amministratore di Sistema.

Antivirus

L'ente si è dotata di un adeguato software antivirus (AVG) che è stato installato su tutti gli strumenti elettronici in dotazione, anche quelli non connessi in rete o ad internet.
L'aggiornamento del prodotto antivirus istallato è continuo va eseguito automaticamente tramite una funzionalità a disposizione nel prodotto stesso.

Gli utenti non devono poter disattivare l'antivirus.
L'antivirus in oggetto controlla in automatico ogni file scaricato dalla rete o dalla posta elettronica o letto da supporti esterni quali floppy disk, cd rom, dvd, etc.
Il personale è stato adeguatamente informato sui comportamenti corretti da tenere per evitare di introdurre virus informatici.
Il Sig. Felcaro Mauro è stato incaricato di seguire il corretto aggiornamento del software antivirus e di eseguire una volta alla settimana un controllo approfondito di tutti i file presenti nel sistema.

Aggiornamento sistema operativo e dei software utilizzati correntemente
Il Sig. Felcaro Mauro è stato incaricato di seguire il corretto aggiornamento del sistema operativo e degli altri software utilizzati, ogni qualvolta la casa produttrice invia gli aggiornamenti.
Onde evitare l'errato utilizzo dei software aggiornati, verranno indette delle attività formative.

Gestione supporti rimovibili contenenti dati particolari
I supporti rimovibili contenenti dati particolari (hard disk, chiavetta usb, cd riscrivibili ecc.), devono essere protetti in appositi armadi e/o classificatori dotati di chiavi. Le chiavi devono essere conservate a cura del responsabile della funzione.
Ogni qualvolta ci sia la necessità di trasferire dati particolari ad altri soggetti bisognerà accertarsi che essi siano autorizzati al trattamento dei dati.
I supporti non devono essere lasciati incustoditi nelle varie postazioni di lavoro, negli ambienti di transito o pubblici, come per esempio corridoi o sale riunioni, etc.
Ad avvenuto trasferimento dei dati i supporti dovranno essere resi illeggibili mediante loro formattazione o mediante loro distruzione fisica (taglio con forbici in più parti, etc.).

Gestione manutenzione strumenti elettronici
La manutenzione degli strumenti elettronici sia a livello hardware sia a livello software viene affidata alla società incaricata della consulenza/assistenza informatica.
In ogni caso non sono stati resi possibili interventi di manutenzione a livello software effettuati via rete a distanza.

Rottamazione sicura delle apparecchiature elettroniche
Al momento di dismettere le apparecchiature ed i supporti (pc, hard disk, cd rom o dvd, chiavette usb, ecc.) ed evitare che rimangano in memoria nomi, indirizzi mail, rubriche telefoniche, foto, filmati, numero di conto bancario, dati personali o particolari, è necessario mettere a punto una serie di misure.
Per dismettere un apparecchio, si deve preoccuparsi di cancellare in maniera definitiva, anche con l'aiuto degli stessi rivenditori o se proprio necessario di tecnici specializzati, tutti i dati personali memorizzati, allo scopo di non esporsi a rischi anche gravi, come ad esempio la manipolazione di dati ed il furto di identità.
È bene proteggere i file usando una password di cifratura, oppure memorizzare i dati su hard disk o su altri supporti magnetici usando sistemi di cifratura automatica al momento della scrittura.
La cancellazione sicura delle informazioni su disco fisso o su altri supporti magnetici è ottenibile con programmi informatici di riscrittura che provvedono, una volta che l'utente abbia eliminato dei file dall'unità disco con i normali strumenti previsti dai sistemi operativi (ad es., con l'uso del cestino o con comandi di cancellazione), a scrivere ripetutamente nelle aree vuote del disco.
Per la distruzione degli hard disk e di supporti magnetici non riscrivibili, come ad esempio cd rom, dvd, penne drive, etc. è consigliabile l'utilizzo di sistemi di punzonatura o deformazione meccanica o di demagnetizzazione ad alta intensità o di vera e propria distruzione fisica.
Si possono anche utilizzare sistemi di formattazione a basso livello degli hard disk o di "demagnetizzazione", in grado di garantire la cancellazione rapida delle informazioni.
Le misure suggerite dal Garante per una rottamazione sicura del pc e di dispositivi elettronici hanno dunque l'obiettivo di richiamare tutti gli utilizzatori sulla necessità di assicurare una reale ed effettiva cancellazione dei dati.

b) Trattamento senza l'ausilio di strumenti elettronici

La documentazione cartacea contenente dati personali deve essere protetta in appositi armadi e/o classificatori dotati di chiavi. Le chiavi devono essere conservate a cura del responsabile della funzione.
Ogni volta che un soggetto autorizzato preleva documenti contenenti dati particolari da tali archivi è tenuto a lasciarne traccia mediante apposita segnalazione riportante il proprio nome, data e ora del prelevamento in un apposito registro.
Tutti i documenti contenenti dati personali o dell'ente che si ritiene debbano essere eliminati devono essere distrutti attraverso appositi "distruggidocumenti" e non gettati nei cestini.
E' vietato il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici, come per esempio corridoi o sale riunioni.
Tutta la documentazione cartacea deve essere riposta negli appositi archivi dopo il suo utilizzo ed i fax cartacei in arrivo o in spedizione non devono essere lasciati incustoditi, così come non devono essere lasciati esposti eventuali documenti sui banconi.

E' estremamente importante prestare la massima attenzione agli argomenti trattati durante le conversazioni telefoniche, se possibile le telefonate e le conversazioni riservate debbono essere differite o effettuate lontano da orecchi indiscreti.
I dati personali o particolari devono essere consegnati preferibilmente nelle mani dell'interessato o di persona delegata per iscritto, la cui delega sia stata controllata. Se risulta impossibile attenersi alle precedenti indicazioni si dovrà avere particolare cura nel ripiegare la missiva in modo che le informazioni non siano visibili all'esterno e la busta dovrà essere chiusa.
Non sono ammesse persone, a qualunque titolo, dopo l'orario di chiusura degli uffici, nei luoghi contenenti gli archivi che custodiscono i dati particolari, se non con previa autorizzazione rilasciata dal titolare della società.
Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura degli uffici, nei luoghi con gli archivi contenenti dati particolari o giudiziari sono identificate e registrate.

11) - Criteri per la protezione delle aree, dei locali e delle infrastrutture di rete

Gli ingressi alla sede dell'ente sono protetti da porte rinforzate, le finestre sono protette da serrande, la sede è dotata anche di un sistema di allarme anti intrusione.
L'accesso fisico alle stanze contenenti documenti trattanti dati personali è permesso solo agli Incaricati del Trattamento Dati.
L'ente si è dotato di un adeguato sistema firewall software e/o router hardware.
Il/I sistema/i è/sono stato/i adeguatamente configurato/i da personale specializzato in sicurezza informatica che ha fornito anche direttive e indicazioni in merito alla sua manutenzione periodica di cui è stato incaricato il signor Felcaro Mauro.

12) - Criteri e modalità per assicurare l'integrità dei dati e la disponibilità in caso di distruzione o danneggiamento

a) Modalità di backup dei dati

Al fine di garantire non solo la integrità, ma anche la pronta disponibilità dei dati l'ente si è dotata di strumenti e procedure di backup.
E' stato scelto un hard disk esterno (unità NAS) per i backup dei dati.
Si è valutata la capienza del supporto, ritenuto più che sufficiente per la mole di dati attualmente gestita.
Tutti i dati personali gestiti con strumenti elettronici vengono inclusi nella procedura di backup.
Tutti i dati personali gestiti con strumenti elettronici vengono inclusi nella procedura di backup. La frequenza con cui vengono effettuate le copie di sicurezza è settimanale, solitamente il venerdì sera.
Il signor Felcaro Mauro è stato incaricato a gestire le copie di sicurezza e le procedure di back up.
Ogni volta viene effettuata una verifica della leggibilità ed integrità del supporto di backup.
Le copie di backup non devono essere conservate nello stesso luogo fisico ove si trovano gli strumenti elettronici con cui si gestiscono i dati personali ma depositate in una cassetta di sicurezza e/o in un luogo adeguato.
Il tempo massimo per la conservazione delle copie di backup è stato stabilito in 2 mesi.
I supporti da eliminare vengono resi inutilizzabili.
Il tempo necessario per recuperare i dati delle copie di sicurezza, a fronte di una generica emergenza, viene stimato in poche ore dal verificarsi del possibile accadimento negativo, comunque ampiamente sotto il limite dei sette giorni previsti dal regolamento, in ipotesi di trattamento di dati particolari.
Con frequenza semestrale dovrà essere effettuata una verifica della leggibilità ed integrità delle copie di sicurezza.

b) Procedure per il ripristino dei dati (restore)

In conseguenza della limitata dimensione e della bassa complessità della struttura dell'ente non si valuta necessario procedere all'elaborazione formale di tali documenti.
Si valuta che le misure di sicurezza attualmente implementate e gestite, esplicitate in questo documento, siano sufficienti per poter ripristinare l'attività ente in tempi brevi e a costi contenuti al verificarsi di emergenze o di eventi negativi.

c) Gruppo di continuità

Al fine di evitare danneggiamenti e quindi attivare le procedure di cui sopra, viene adottato un adeguato gruppo di continuità "UPS" per prevenire le conseguenze dei blackout elettrici o dei picchi di sovra o sotto tensione elettrica.
Il gruppo di continuità in oggetto è in grado di fornire energia elettrica per un tempo sufficiente per attivare tutte le procedure di spegnimento.

13) - La previsione di interventi formativi per gli Incaricati del Trattamento

L'ente riconosce l'importanza della formazione dei suoi componenti riguardo le tematiche della privacy, come elemento significativo di protezione del proprio sistema informativo e s'impegna a promuovere momenti formativi, in particolare al momento

dell'assunzione o al momento di cambiamenti di mansioni o all'introduzione di nuovi strumenti elettronici che hanno impatto sul trattamento dei dati personali.
Tutti i componenti dell'ente devono comunque partecipare una volta all'anno ad un corso/incontro di approfondimento e mantenimento delle conoscenze in materia di sicurezza informatica in aula o in modalità e-learning.

14) - Criteri per garantire l'adozione delle misure minime nel caso di trattamenti affidati all'esterno della struttura aziendale

I dati necessari per l'elaborazione di paghe e contributi, elaborazione di documenti fiscali e dichiarazioni dei redditi, attività di medicina e sicurezza sul lavoro, etc., sono tenuti presso gli studi e/o le società di consulenza che hanno rilasciato una dichiarazione scritta in cui certificano che presso la loro sede sono state implementate e sono operative le misure di sicurezza minime richieste dal Regolamento europeo 2016/679.
Nell'ipotesi vi fosse necessità di affidare trattamenti temporanei di dati personali all'esterno, per esempio ad altri professionisti e/o società, va richiesta a tali soggetti una dichiarazione scritta in cui viene certificata la conformità del loro sistema informativo alle previsioni della normativa sulla protezione dei dati "privacy".

15) - Modalità di aggiornamento del Registro del Trattamento

Il Titolare del Trattamento è il soggetto preposto all'aggiornamento e alla custodia del Registro dei Trattamento.

Il documento in oggetto non deve rimanere statico ma deve essere aggiornato ogni volta che vi siano cambiamenti significativi nell'ente impattanti sulle misure minime di sicurezza.

In caso di modifiche sostanziali o comunque ogni tre anni, il Titolare del Trattamento procederà alla revisione del documento in oggetto.

Manzano, lì 15/05/2018

Il Titolare del Trattamento
Mauro Felcaro il 15/05/2018 12:07
Firma digitale ai sensi dell'artt.20,21,23,24 del D.Lgs.82/05 s.m.i.
Riproduzione cartacea del documento informatico originale

Firme per attribuzione di data certa L.325/2000, artt. 2702, 2704 C.C.

- Appendice: Alcuni articoli del Regolamento

Di seguito sono riportati alcuni articoli del Regolamento europeo 2016/679 del 27 aprile 2016 al fine di portare a conoscenza degli addetti/incaricati al trattamento gli aspetti salienti del nuovo Regolamento che possono coinvolgerli nell'espletamento della loro operatività giornaliera.
Si tiene a specificare che il testo completo del Regolamento suddetto è a disposizione di coloro che sono interessati a prenderne visione presso la sede della società in formato elettronico e/o cartaceo, previa specifica richiesta.

DISPOSIZIONI GENERALI

Articolo 1
Oggetto e finalità

1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.
2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Articolo 4
Definizioni

Ai fini del presente regolamento s'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) «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;
3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
4) «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;
5) «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;
6) «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;
7) «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;
8) «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;
9) «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;
10) «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;
11) «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;

12) «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;
13) «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;
14) «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;
15) «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;
16) «stabilimento principale»:
a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;
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'artico lo 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) «trattamento transfrontaliero»:
a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
24) «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;
25) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento Europeo e del Consiglio;
26) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

PRINCIPI

Articolo 6
Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

2. Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX.
3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:
a) dal diritto dell'Unione; o
b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento. La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.
4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:
a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;
d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Articolo 7
Condizioni per il consenso

1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.
Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

DIRITTI DELL'INTERESSATO

Articolo 12
Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.
2. Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22. Nei casi di cui all'articolo 11, paragrafo 2, il titolare del trattamento non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 15 a 22, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'interessato.
3. Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.
4. Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.
5. Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:
a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
b) rifiutare di soddisfare la richiesta. Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.
6. Fatto salvo l'articolo 11, qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 15 a 21, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.
7. Le informazioni da fornire agli interessati a norma degli articoli 13 e 14 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.
8. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 92 al fine di stabilire le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate.

Articolo 13
Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.
2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:
a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di proporre reclamo a un'autorità di controllo;
e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.
4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

Articolo 14
Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni:
a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) le categorie di dati personali in questione;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.
2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:
a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
e) il diritto di proporre reclamo a un'autorità di controllo;
f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2:
a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.
4. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2.
5. I paragrafi da 1 a 4 non si applicano se e nella misura in cui:
a) l'interessato dispone già delle informazioni;
b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure
d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

Articolo 17
Diritto alla cancellazione («diritto all'oblio»)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragr.1.
2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO

Articolo 24
Responsabilità del titolare del trattamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.
2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.
3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Articolo 26
Contitolari del trattamento

1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.
2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
3. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

Articolo 28
Responsabile del trattamento

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.
2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.
3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.
Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:
a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'articolo 32;
d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e
h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.
4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.
5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.
6. Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43.
7. La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.
8. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63.
9. Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.
10. Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

Articolo 30
Registri delle attività di trattamento

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;
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.
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.
3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.
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.
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.

Articolo 32
Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti 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.

Articolo 33
Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Articolo 34
Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Articolo 35
Valutazione d'impatto sulla protezione dei dati

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.
3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.
5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.
6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.
7. La valutazione contiene almeno:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.
9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.
10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.
11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Articolo 37
Designazione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:
a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.
2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.
3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.
4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.
5. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti dell'articolo 39.
6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.
7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Articolo 38
Posizione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.
4 Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.
6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

Articolo 39
Compiti del responsabile della protezione dei dati

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:
a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento 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;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo; e
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

TRASFERIMENTI DI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI

Articolo 44
Principio generale per il trasferimento

Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato.

Articolo 44
Trasferimento sulla base di una decisione di adeguatezza

1. Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.
2. Nel valutare l'adeguatezza del livello di protezione, la Commissione prende in considerazione in particolare i seguenti elementi:
a) lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza nonché i diritti effettivi e azionabili degli interessati e un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento;
b) l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale, con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati, comprensiva di adeguati poteri di esecuzione, per assistere e fornire consulenza agli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo degli Stati membri; e
c) gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali.
3. La Commissione, previa valutazione dell'adeguatezza del livello di protezione, può decidere, mediante atti di esecuzione, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo. L'atto di esecuzione prevede un meccanismo di riesame periodico, almeno ogni quattro anni, che tenga conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale.

L'atto di esecuzione specifica il proprio ambito di applicazione geografico e settoriale e, ove applicabile, identifica la o le autorità di controllo di cui al paragrafo 2, lettera b), del presente articolo. L'atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.
4. La Commissione controlla su base continuativa gli sviluppi nei paesi terzi e nelle organizzazioni internazionali che potrebbero incidere sul funzionamento delle decisioni adottate a norma del paragrafo 3 del presente articolo e delle decisioni adottate sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46/CE.
5. Se risulta dalle informazioni disponibili, in particolare in seguito al riesame di cui al paragrafo 3 del presente articolo, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale non garantiscono più un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, la Commissione revoca, modifica o sospende nella misura necessaria la decisione di cui al paragrafo 3 del presente articolo mediante atti di esecuzione senza effetto retroattivo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2, o, in casi di estrema urgenza, secondo la procedura di cui all'articolo 93, paragrafo 3.
Per imperativi motivi di urgenza debitamente giustificati, la Commissione adotta atti di esecuzione immediatamente applicabili secondo la procedura di cui all'articolo 93, paragrafo 3.
6. La Commissione avvia consultazioni con il paese terzo o l'organizzazione internazionale per porre rimedio alla situazione che ha motivato la decisione di cui al paragrafo 5.
7. Una decisione ai sensi del paragrafo 5 del presente articolo lascia impregiudicato il trasferimento di dati personali verso il paese terzo, il territorio o uno o più settori specifici all'interno del paese terzo, o verso l'organizzazione internazionale in questione, a norma degli articoli da 46 a 49.
8. La Commissione pubblica nella Gazzetta ufficiale dell'Unione UEropea e sul suo sito web l'elenco dei paesi terzi, dei territori e settori specifici all'interno di un paese terzo, e delle organizzazioni internazionali per i quali ha deciso che è o non è più garantito un livello di protezione adeguato.
9. Le decisioni adottate dalla Commissione in base all'articolo 25, paragrafo 6, della direttiva 95/46/CE restano in vigore fino a quando non sono modificate, sostituite o abrogate da una decisione della Commissione adottata conformemente al paragrafo 3 o 5 del presente articolo.

SANZIONI

Articolo 83
Condizioni generali per infliggere sanzioni amministrative pecuniarie

1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.
2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:
a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
b) il carattere doloso o colposo della violazione;
c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;
e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
g) le categorie di dati personali interessate dalla violazione;
h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e
k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.
3. Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.
4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:
a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;
b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;
5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:
a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;
b) i diritti degli interessati a norma degli articoli da 12 a 22;
c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;
d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;
e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.
6. In conformità del paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.
7. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.
8. L'esercizio da parte dell'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo.
9. Se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, il presente articolo può essere applicato in maniera tale che l'azione sanzionatoria sia avviata dall'autorità di controllo competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni effettive, proporzionate e dissuasive. Tali Stati membri notificano alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro 25 maggio 2018 e comunicano senza ritardo ogni successiva modifica.

- Allegato 1 – Istruzioni di utilizzo degli strumenti elettronici

ISTRUZIONI DI UTILIZZO DEGLI STRUMENTI ELETTRONICI

Premessa
I dipendenti, collaboratori e i soci dell'ente devono ispirarsi ad un principio generale di diligenza e correttezza nell'utilizzo delle risorse informatiche, telematiche e del patrimonio informativo della società.
Ogni utilizzo del sistema informativo diverso da finalità strettamente professionali è espressamente vietato.
Di seguito vengono esposte regole minime comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine della società stessa.
L'ente s'impegna a formare gli incaricati in merito ai rischi, alle procedure operative, alla prevenzione dei danni e, più in generale, alle problematiche relative alla sicurezza in materia di trattamento dei dati.
Il regolamento deve essere portato a conoscenza e distribuito a tutti i componenti dell'ente.

Utilizzo dell'elaboratore e della rete interna
Tutti i supporti magnetici devono essere utilizzati previa autorizzazione dell'Ente.
L'accesso all'elaboratore della propria postazione di lavoro, sia esso collegato in rete o "stand alone", è protetto da un sistema di autenticazione.
La password assegnata non deve essere divulgata e deve essere custodita dall'assegnatario con la massima diligenza.
E' vietato istallare qualsiasi software anche demo e/o in forma provvisoria, senza autorizzazione.
Su ogni elaboratore dell'ente è stato installato un software antivirus per prevenire eventuali danneggiamenti all'hardware o al software causati dalla presenza o dall'azione di programmi virus informatici.
E' importante utilizzare questi software antivirus per controllare qualsiasi file di provenienza esterna.
Si ricorda che nonostante la presenza del software antivirus è possibile che riescano ugualmente ad installarsi nei computer virus informatici non identificati o riconoscibili.
Pertanto in caso si evidenzino anomalie di funzionamento del computer è importante darne rapida segnalazione al Titolare del Trattamento.
Le unità di rete e le aree di condivisione contengono informazioni strettamente professionali e non possono essere utilizzate per scopi diversi.
Non bisogna dislocare stampanti e fax in aree accessibili a soggetti non abilitati al trattamento e non presidiate (ad esempio i corridoi degli uffici).

Utilizzo servizi vari su internet
I servizi on line devono essere esclusivamente finalizzati al reperimento di informazioni utili all'ente.
Ogni altra utilizzazione dell'accesso su internet, non finalizzata al reperimento di informazioni utili all'attività dell'Ente, non pertinente all'attività lavorativa o di tipo personale non è consentita.
Al fine di non compromettere la sicurezza della società e di prevenire conseguenze legali o di altro genere a carico dell'ente, gli utenti dovranno adottare i seguenti comportamenti:

- evitare lo scaricamento di programmi software, anche gratuiti, se non per esigenze strettamente professionali e fatti comunque salvi i casi di esplicita autorizzazione;
- è vietata la partecipazione a Forum non professionali, l'utilizzo di chat , di bacheche elettroniche e, più in generale, qualunque utilizzo di servizi Internet, attuali o futuri, non strettamente inerenti all'attività professionale.

Utilizzo del servizio di posta elettronica
Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità dell'ente ed in stretta connessione con l'effettiva attività e mansioni del soggetto dipendente e/o collaboratore che utilizza tale funzionalità.
Non è possibile utilizzare tale servizio per finalità in contrasto con quelle della società, o non pertinenti all'attività lavorativa o personali.
Al fine di non compromettere la sicurezza dell'ente e di prevenire conseguenze legali a carico della società stessa bisogna adottare le seguenti norme comportamentali:

- se nonostante i controlli preventivi antispamming e antivirus automatici, si ricevono mail da destinatari sconosciuti contenenti file (in particolare programmi eseguibili o file di word processor e fogli di calcolo contenenti delle macro, file compressi, etc.) evitare di aprire tali mail e tali file e procedere alla loro immediata eliminazione. Il comportamento sopradescritto va seguito anche se si ricevono file non concordati da destinatari conosciuti;
- è fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list salvo diversa ed esplicita autorizzazione;
- la casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.

Si precisa che in caso di assenza del dipendente la continuità dell'attività lavorativa sarà comunque garantita dalla nomina di un fiduciario per la lettura dei messaggi.
Si precisa che il Datore di Lavoro potrà effettuare, ai sensi di legge, controlli e verifiche, anche saltuari ed occasionali, sulla sicurezza e funzionalità del sistema, con preventiva indicazione delle relative specifiche, ragioni e modalità.
Resta inteso che, in caso di abusi singoli o reiterati, verranno effettuati controlli nominativi o su singoli dispositivi o postazioni, e ciò ai sensi di legge.
La inosservanza delle prescrizioni, comprese quelle sopraindicate, comporterà l'applicazione delle sanzioni disciplinari previste al vigente contratto di lavoro.

Gestione dei documenti cartacei
La documentazione cartacea contenente dati personali o particolari deve essere protetta in appositi armadi e/o classificatori dotati di chiavi. Le chiavi devono essere conservate a cura del responsabile della funzione.
Ogni volta che un soggetto autorizzato preleva documenti contenenti dati particolari da tali archivi è tenuto a lasciarne traccia mediante apposita segnalazione riportante il proprio nome, data e ora del prelevamento in un apposito registro.
Tutti i documenti contenenti dati personali o dell'ente che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.
E' vietato il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici, come per esempio corridoi o sale riunioni.
Tutta la documentazione cartacea deve essere riposta negli appositi archivi dopo il suo utilizzo ed i fax cartacei in arrivo o in spedizione non devono essere lasciati incustoditi, così come non devono essere lasciati esposti eventuali documenti sui banconi.
E' estremamente importante prestare la massima attenzione agli argomenti trattati durante le conversazioni telefoniche, se possibile le telefonate e le conversazioni riservate debbono essere differite o effettuate lontano da orecchi indiscreti.
I dati personali o particolari devono essere consegnati preferibilmente nelle mani dell'interessato o di persona delegata per iscritto, la cui delega sia stata controllata. Se risulta impossibile attenersi alle precedenti indicazioni si dovrà avere particolare cura nel ripiegare la missiva in modo che le informazioni non siano visibili all'esterno e la busta dovrà essere chiusa.
Non sono ammesse persone, a qualunque titolo, dopo l'orario di chiusura degli uffici, nei luoghi contenenti gli archivi che custodiscono i dati particolari, se non con previa autorizzazione rilasciata dal titolare della società.
Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura degli uffici, nei luoghi con gli archivi contenenti dati particolari o giudiziari sono identificate e registrate.

Dichiarazione di presa visione istruzioni di utilizzo:

Il/La sottoscritto/a …….. dichiara di aver preso piena visione e di aver ricevuto copia delle "Istruzioni di utilizzo degli strumenti elettronici" dell'ente e s'impegna al pieno rispetto di tali norme comportamentali.

……..……., lì …… In fede ……..

- Allegato 2 – Istruzioni sistema di identificazione, autenticazione e gestione password

ISTRUZIONI SISTEMA DI IDENTIFICAZIONE, AUTENTICAZIONE E GESTIONE PASSWORD

L'ente ha attivato ed è correntemente funzionante un sistema d'autenticazione per ognuno degli incaricati che trattano dati personali.
E' stato attribuito un codice identificativo (username, user ID) strettamente personale per l'utilizzazione degli strumenti elettronici (di solito personal computer) del sistema informatico.
Ad ogni incaricato possono eventualmente essere assegnati più codici per l'identificazione, ad esempio per funzioni diverse.
I codici identificativi sono frequentemente aggiornati, inserendo quelli dei nuovi incaricati e cancellando quelli degli incaricati non più autorizzati.
Il sistema di autenticazione prevede l'utilizzo di parole chiave (password) sia a livello di sistema operativo sia a livello di singola applicazione.
Le password da utilizzare devono:

- essere diverse da parole presenti nei vocabolari;
- non fare riferimento con informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro familiari;
- contenere una combinazione di numeri e lettere, maiuscole e minuscole.

Il Titolare del Trattamento è incaricato della gestione delle password dell'ente.
Non bisogna:

- rivelare la password a nessuno, soprattutto attraverso il telefono;
- scrivere la password in un messaggio di posta elettronica, o su supporti cartacei conservati in ufficio;
- rivelare o condividere la password con i colleghi di lavoro, famigliari e amici;
- utilizzare la caratteristica, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni;
- archiviare la password su un qualsiasi strumento elettronico, incluso il telefono cellulare, o su supporti cartacei conservati in ufficio, senza utilizzare un sistema di crittografia.

Viene segnalato agli incaricati che la lunghezza della password da utilizzare non deve essere inferiore ad otto caratteri, salvo limitazioni tecniche nei software in uso.
Si sollecita l'incaricato che riceve una password a modificarla al primo utilizzo.
L'incaricato deve segnalare al Titolare del Trattamento la sua password in uso che l'annota su un registro cartaceo conservato nella cassetta di sicurezza della banca e/o altro luogo adeguato.
Inoltre il sostituto dell'Incaricato al Trattamento dei dati deve essere messo in grado di poter lavorare sulla postazione di colui che sta sostituendo comunicandogli la password e l'id, in seguito a tale comunicazione è pertanto obbligato a rispettare il regolamento suddetto per quanto riguarda la selezione e gestione della password.
Viene segnalato ad ogni incaricato la necessità di cambiare la password almeno ogni 6 mesi. Nell'ipotesi di trattamento di dati particolari viene segnalato ad ogni incaricato la necessità di cambiare la password almeno ogni 3 mesi. E' prevista una scadenza nella validità di ogni password utilizzata. Sono vietate credenziali di autenticazione (username e password) condivise fra più persone. Le credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate. Le credenziali di autenticazione vengono immediatamente revocate in caso di provvedimenti disciplinari o quando si presentano situazioni che possono compromettere la sicurezza.
La visualizzazione della password sullo schermo dei personal computer è impedita da tutti i software in uso.
Il sistema di identificazione ed autenticazione è operativo anche sui computer portatili e sui palmari che possono gestire e contenere dati personali.

Dichiarazione di presa visione delle "Istruzioni sistema di identificazione e autenticazione e gestione password":

Il/La sottoscritto/a …….. dichiara di aver preso piena visione e di aver ricevuto copia delle "Istruzioni sistema di identificazione e autenticazione e gestione password" e s'impegna al pieno rispetto di tali norme comportamentali.

……., lì …… In fede ……..

- Allegato 3 – Lettera di nomina Responsabile del Trattamento

Nomina Responsabile del Trattamento

Il sottoscritto ....., in qualità di legale rappresentante dell'ente……, Titolare, ai sensi dell'art.4, comma 7), del RE 2016/679,

NOMINA

Ella, Sig. …….. RESPONSABILE DEL TRATTAMENTO a tutti gli effetti legali, secondo i criteri, le modalità e le istruzioni di seguito specificate.

Ella ha l'obbligo di operare secondo le istruzioni impartite dal titolare e di fornire al medesimo tutte le informazioni e garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti del presente Regolamento e garantisca il mantenimento dei livelli minimi di sicurezza e la tutela dei diritti dell'interessato.
Si valuta che Ella sia in possesso dei requisiti di esperienza, capacità ed affidabilità richiesti dalle norme vigenti.

Ella in particolare dovrà:

- trattare i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, dovrà informare il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adottare scrupolosamente tutte le misure di sicurezza previste dal regolamento consapevole che la loro corretta applicazione è condizione necessaria per non vanificare le misure e le procedure implementate dal nostro ente nel campo della sicurezza del trattamento dei dati personali;
- rispettare le condizioni per ricorrere a un altro responsabile del trattamento richiedendo autorizzazione scritta, specifica o generale, del titolare del trattamento;
- tenere conto della natura del trattamento, assistere il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del presente Regolamento, tenendo conto della natura del trattamento e delle informazioni a disposizione;
- su scelta del titolare del trattamento, cancellare o restituire tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti;
- mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente Regolamento e consentire e contribuire alle attività di revisione.

Luogo e data …….. Il Titolare del Trattamento .....

Per presa visione e integrale accettazione

Il Responsabile del Trattamento .....

- Allegato 4 – Lettera di nomina Addetto al Trattamento

Nomina Addetto al Trattamento

Egr. Sig. / Gent.ma…….. nella Sua qualità di ……..…… *(indicare ruolo e mansioni),* Lei svolge anche operazioni riguardanti il trattamento di dati personali.

In particolare, le banche dati a cui può accedere sono: ……

In ottemperanza alle previsioni del RE 2016/679, Lei viene designato/a:

ADDETTO AL TRATTAMENTO

In questo ruolo e nei limiti delle mansioni a Lei affidate, potrà eseguire le operazioni di trattamento riguardanti le sopraddette banche dati, attenendosi alle istruzioni impartite dal Titolare del Trattamento.

In linea generale Le è fatto comunque assoluto divieto di comunicazione e divulgazione di qualsivoglia dato gestito dalla società.

In particolare, in riferimento alla sicurezza del trattamento dei dati disciplinata dagli articoli del regolamento, Le vengono fornite, in allegato, le istruzioni operative che avrà cura di osservare con la dovuta attenzione, consapevole che la loro scrupolosa applicazione è condizione necessaria per non vanificare le misure e le procedure implementate dalla società nel campo della sicurezza del trattamento dei dati personali.

La presente sostituisce qualunque precedente comunicazione in materia.

La invitiamo a restituire la presente comunicazione debitamente sottoscritta in segno di ricevuta e integrale accettazione.

Firma del Titolare del Trattamento .....

Per accettazione incarico

Data e Firma…….....

Dichiarazione di presa visione regolamento di utilizzo

Dichiaro di aver preso visione del Registro dei Trattamenti e mi impegno al pieno rispetto delle citate norme comportamentali.

Data e Firma ……..……

- Allegato 5 – Lettera di nomina Responsabile del Trattamento "Esterno"

Nomina Responsabile del Trattamento "Esterno"

Spett.le ……., nell'espletamento dell'incarico professionale conferitoLe, Lei svolge anche operazioni riguardanti il trattamento di dati personali dei quali è titolare il nostro ente.

In particolare, le banche dati a cui può accedere sono: ……

In ottemperanza alle previsioni del Regolamento Europeo 2016/679, a tutti gli effetti legali, secondo i criteri, le modalità e le istruzioni di seguito specificate Lei viene designato:

RESPONSABILE DEL TRATTAMENTO

In questo ruolo, potrà svolgere tutte le operazioni necessarie all'espletamento del Suo mandato attingendo informazioni dalle banche dati sopra menzionate, Le è fatto, comunque, assoluto divieto di comunicazione e divulgazione di qualsivoglia dato di cui è venuto a conoscenza se non previa nostra autorizzazione.

Ella ha l'obbligo di operare secondo le istruzioni impartite dal titolare e di fornire al medesimo tutte le informazioni e garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti del presente Regolamento e garantisca il mantenimento dei livelli minimi di sicurezza e la tutela dei diritti dell'interessato.

Si valuta che Ella sia in possesso dei requisiti di esperienza, capacità ed affidabilità richiesti dalle norme vigenti.

In particolare dovrà:

- trattare i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, dovrà informare il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza. Precisiamo che è tenuto ad informare correttamente i Suoi incaricati e a garantire il rispetto delle misure minime di sicurezza;
- adottare scrupolosamente tutte le misure di sicurezza previste dal regolamento consapevole che la loro corretta applicazione è condizione necessaria per non vanificare le misure e le procedure implementate dal nostro ente nel campo della sicurezza del trattamento dei dati personali;
- rispettare le condizioni per ricorrere a un altro responsabile del trattamento richiedendo autorizzazione scritta, specifica o generale, del titolare del trattamento;
- tenere conto della natura del trattamento, assistere il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del presente Regolamento, tenendo conto della natura del trattamento e delle informazioni a disposizione;
- su scelta del titolare del trattamento, cancellare o restituire tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti;
- mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente Regolamento e consentire e contribuire alle attività di revisione.

Firma del Titolare del Trattamento ……

La invitiamo a restituire la presente comunicazione debitamente sottoscritta in segno di ricevuta e integrale accettazione.

Data e firma ……

- Allegato 6 – Lettera di nomina Responsabile del Trattamento "Esterno" (attività di pulizia)

Nomina Responsabile del Trattamento "Esterno" (attività di pulizia)

Spett.le ....., nell'espletamento della Vs. attività di pulizia, Voi casualmente potreste venire a contatto con documenti appartenenti alla ns. ditta che potrebbero contenere dati personali e/o particolari dei quali è titolare la nostra ente.

In ottemperanza alle previsioni del Regolamento Europeo 2016/679, a tutti gli effetti legali, secondo i criteri, le modalità e le istruzioni di seguito specificate Lei viene designato:

RESPONSABILE DEL TRATTAMENTO

In questo ruolo, potrete svolgere tutte le operazioni necessarie all'espletamento della Vs. attività di pulizia, Vi è fatto, comunque, assoluto divieto di comunicazione e divulgazione di qualsivoglia dato di cui potreste venire casualmente a conoscenza.

Ricordiamo inoltre l'importanza di informare correttamente tutti i Vs. incaricati nel caso vengano casualmente a conoscenza di dati personali e/o particolari appartenenti alla ns. società.

In particolare, in riferimento alla sicurezza del trattamento dei dati, Vi viene richiesto di adottare scrupolosamente tutte le misure di sicurezza minime obbligatorie previste dal regolamento, consapevoli che la loro corretta applicazione è condizione necessaria per non vanificare le misure e le procedure implementate dalla nostra ente nel campo della sicurezza del trattamento dei dati personali.

Firma del Titolare del Trattamento ……..……

La invitiamo a restituire la presente comunicazione debitamente sottoscritta in segno di ricevuta e integrale accettazione.

Data e firma……

- Allegato 7 – Informativa trattamento dati personali

Egregio sig. / Gent.ma sig.ra-ina
cognome e nome .....
Interessato/a al trattamento

OGGETTO: *informativa e richiesta di consenso ai sensi del Regolamento Europeo 2016/679, relativo alla tutela del trattamento dei dati personali.*

La scrivente La/Vi informa ai sensi e per gli effetti dell'art.13 del RE 2016/679:

1) Per l'instaurazione e l'esecuzione dei rapporti contrattuali con Lei/Voi in corso è in possesso di dati particolari acquisiti anche verbalmente direttamente e/o tramite terzi.

2) Il suddetto Regolamento Europeo prevede una serie di obblighi in capo a chi effettua "trattamenti" (cioè raccolta, registrazione, elaborazione, conservazione, comunicazione, diffusione, ecc.) di dati personali riferiti ad altri soggetti.

3) Il trattamento dei Suoi dati personali e di quelli dei Suoi familiari di cui siamo in possesso o che Le/Vi saranno richiesti o che ci verranno comunicati da Lei/Voi o da terzi è svolto/sarà svolto in esecuzione degli obblighi legali e contrattuali relativi al rapporto di lavoro subordinato:
   - in corso dal .....

4) In particolare, il trattamento dei Suoi dati personali e di quelli dei Suoi familiari sarà svolto ai fini di:
   - elaborazione e pagamento delle retribuzioni e di ogni altro emolumento in denaro o in natura previsto dalla legge, da contratti collettivi o individuali;
   - adempimento degli obblighi di legge o di contratto nei confronti degli istituti previdenziali, assistenziali, assicurativi, anche a carattere integrativo;
   - adempimenti fiscali e comunicazioni all'amministrazione finanziaria, ivi compresa l'eventuale l'assistenza fiscale (modello Unico, ecc.);
   - adempimenti relativi alle norme in materia di sicurezza sul lavoro (D.Lgs.81/08);
   - registrazioni ai fini della legislazione sul lavoro, civilistica e fiscale.

5) Le suddette finalità possono comportare la necessità/opportunità di trattare dati personali relativi ad altri soggetti (es. coniuge, figli, persone a carico).

6) Il trattamento avverrà con sistemi manuali e/o elettronici atti a memorizzare, gestire e trasmettere i dati stessi, con logiche strettamente correlate alle finalità stesse, sulla base dei dati in nostro possesso e con impegno da parte Sua/Vostra di comunicarci tempestivamente eventuali correzioni, integrazioni e/o aggiornamenti.

7) I Suoi/Vostri dati, per obblighi di legge o per esclusive ragioni funzionali nell'ambito dell'esecuzione del contratto, verranno comunicati:
   - ai professionisti esterni di cui ci avvaliamo;
   - a enti pubblici e privati con finalità previdenziali, assistenziali o assicurative, anche integrative - specificare i soggetti (es. INPS, INAIL, Ispettorato del Lavoro, ASL, ecc.);
   - a soggetti che possono accedere ai Suoi/Vostri dati in forza di disposizioni di legge o di normativa secondaria o comunitaria;
   - altri soggetti (es. società, enti o associazioni con finalità sportive, culturali, ricreative, altri soggetti potenzialmente interessati ad una ricerca di personale, ecc.).

8) L'ambito di eventuale comunicazione dei dati sarà entro la Comunità Europea.

9) Il conferimento dei dati da parte Sua/Vostra ha natura obbligatoria e i dati sono indispensabili per l'adempimento degli obblighi legali o contrattuali derivanti dal contratto in corso o da eventuali futuri rapporti. I dati personali da Lei conferiti verranno conservati fino ad una eventuale risoluzione del rapporto di lavoro in essere e per successivi 10 anni come da disposizioni normative;

10) In caso di Suo/Vostro rifiuto a conferire i dati, a consentire al loro trattamento e alla loro comunicazione ai suddetti soggetti può derivare:
- l'impossibilità di adempiere a operazioni anche di Suo/Vostro diretto interesse, quali ad esempio:
  - elaborare le retribuzioni ed effettuare i relativi adempimenti previdenziali e assistenziali;
  - adempiere ai previsti obblighi fiscali (es. ritenute d'imposta, certificazione degli emolumenti corrisposti);
- la possibile irrogazione di sanzioni.

11) Il Titolare del Trattamento è l'ente ..... nella persona del Legale Rappresentante pro tempore ivi domiciliato.

12) I Responsabili Trattamento "Esterni" sono i seguenti soggetti:

Ragione Sociale	Indirizzo

13) Nei Suoi/Vostri confronti è previsto l'esercizio di alcuni diritti, in particolare:
- conoscere l'esistenza o meno di dati personali che La/Vi riguardano e la loro comunicazione in forma intellegibile;
- essere informato sul titolare, sulle finalità e sulle modalità del trattamento e sull'eventuale responsabile, sui soggetti o categorie di soggetti ai quali i dati personali possono essere comunicati;
- ottenere l'accesso, l'aggiornamento, la rettificazione o l'integrazione dei dati;
- ottenere la cancellazione, la trasformazione in forma anonima o il blocco degli stessi;
- opporsi per motivi legittimi al trattamento dei dati, salvi i limiti stabiliti dalla legge;
- opporsi all'invio di materiale pubblicitario o per il compimento di ricerche di mercato o di comunicazione commerciale;
- revocare il consenso in qualsiasi momento;
- proporre reclamo all'autorità di controllo;

Il testo completo del Regolamento Europeo 2016/679 relativo ai diritti dell'interessato è disponibile in ente presso l'ufficio del Responsabile della Privacy e sul sito *www.garanteprivacy.it*.

La/Vi preghiamo quindi di volere esprimere il Suo/Vostro consenso scritto ai predetti trattamenti e alle conseguenti comunicazioni e/o diffusioni, nonché il Suo/Vostro impegno a comunicarci tempestivamente le eventuali variazioni dei dati in nostro possesso, facendoci pervenire con cortese sollecitudine copia del consenso per accettazione e conferma.

- Allegato 8 – Consenso dell'interessato al trattamento dei dati personali

CONSENSO DELL'INTERESSATO/I AL TRATTAMENTO DI DATI PERSONALI

Il/La sottoscritto/a ……, pienamente informato ai sensi dell'art.13 del RE 2016/679 sul trattamento dei miei/nostri dati personali, ai sensi dell'art.7 dello stesso:

- per quanto riguarda il trattamento dei miei/nostri dati personali "particolari", nei limiti in cui sia strumentale per le finalità perseguite dal trattamento:

  ☐ esprimo / esprimiamo il consenso ☐ nego / neghiamo il consenso

- per quanto riguarda la comunicazione dei dati personali a soggetti che svolgono attività funzionalmente collegate all'esecuzione del rapporto di lavoro, quali:
  - professionisti esterni di cui ci avvaliamo;
  - enti pubblici e privati con finalità previdenziali, assistenziali o assicurative, anche integrative (ad es. INPS, INAIL, Ispettorato del Lavoro, ASL, ecc.);
  - soggetti che possono accedere ai Suoi/Vostri dati in forza di disposizioni di legge o di normativa secondaria o comunitaria;

  ☐ esprimo / esprimiamo il consenso ☐ nego / neghiamo il consenso

- per quanto riguarda la comunicazione dei dati personali a soggetti che svolgono attività non funzionalmente collegate al rapporto di lavoro:
  - società, enti o associazioni con finalità sportive, culturali, ricreative, altri soggetti potenzialmente interessati ad una ricerca di personale, etc.:

  ☐ esprimo / esprimiamo il consenso ☐ nego / neghiamo il consenso

Sarà mio/nostro impegno comunicarvi tempestivamente le eventuali modifiche, variazioni e/o integrazioni dei dati in vostro possesso.

Data ..... Firma dell'interessato per consenso …….....

- Allegato 9 – Informativa a clienti e fornitori

INFORMATIVA PER IL TRATTAMENTO DI DATI PERSONALI

Spett.le Cliente/Fornitore
Loro sede

OGGETTO: *informativa ai sensi dell'art.13 del RE 2016/679, relativo alla tutela del trattamento dei dati personali.*

Con la presente, Vi informiamo:

1) il suddetto Regolamento prevede una serie di obblighi in capo a chi effettua "trattamenti" (cioè raccolta, registrazione, elaborazione, conservazione, comunicazione, diffusione, ecc.) di dati personali riferiti ad altri soggetti;
2) il trattamento dei Vostri dati di cui siamo in possesso o che Vi saranno richiesti o che ci verranno comunicati sarà svolto in esecuzione di:
   - obblighi legali (es. fatturazione, scritture e registrazioni contabili obbligatorie, società di consulenza, società di revisione, società di certificazione, etc.);
   - obblighi contrattuali (es. rapporti di acquisto/vendita, rapporti con istituti di credito, mandato professionale, etc.);
   - altre finalità (es. ricerche potenziali clienti/fornitori, indagini di mercato, etc.);
3) in occasione di tali trattamenti potremmo venire a conoscenza di dati che il RE 2016/679 definisce "personali";
4) il trattamento avverrà con sistemi manuali e/o elettronici atti a memorizzare, gestire e trasmettere i dati stessi, con logiche strettamente correlate alle finalità stesse, sulla base dei dati in nostro possesso e con impegno da parte Vostra di comunicarci tempestivamente eventuali correzioni, integrazioni e/o aggiornamenti;
5) i dati potranno essere comunicati in Italia e/o nell'ambito della Comunità Europea, esclusivamente per le finalità sopra indicate;
6) in caso di Vostro rifiuto a conferire i dati o a consentire al loro trattamento ovvero alla loro comunicazione ne potrà derivare:
   - l'impossibilità di instaurare o proseguire il rapporto, ovvero di effettuare alcune operazioni, se i dati sono necessari all'esecuzione del rapporto o dell'operazione;
   - l'impossibilità di effettuare alcune operazioni che presuppongono la comunicazione dei dati a soggetti funzionalmente collegati all'esecuzione delle stesse;
7) nei Vostri confronti è previsto l'esercizio di alcuni diritti, in particolare di:
   - conoscere l'esistenza o meno di dati personali che La/Vi riguardano e la loro comunicazione in forma intellegibile;
   - essere informato sul titolare, sulle finalità e sulle modalità del trattamento e sull'eventuale responsabile, sui soggetti o categorie di soggetti ai quali i dati personali possono essere comunicati;
   - ottenere l'aggiornamento, la rettificazione o l'integrazione dei dati;
   - ottenere la cancellazione, la trasformazione in forma anonima o il blocco degli stessi;
   - opporsi per motivi legittimi al trattamento dei dati, salvi i limiti stabiliti dalla legge;
   - opporsi all'invio di materiale pubblicitario o per il compimento di ricerche di mercato o di comunicazione commerciale;
8) I Vostri dati personali verranno conservati fino ad un periodo massimo di 10 anni, fatto salvo il diritto alla cancellazione o all'oblio ai sensi dell'art.17, che potrà essere sempre esercitato.

Il Titolare del Trattamento è l'ente …… nella persona del Legale Rappresentante pro tempore ivi domiciliato.

Timbro Firma ……

- Allegato 10 – Consenso al Trattamento dei dati clienti e fornitori

CONSENSO PER IL TRATTAMENTO DI DATI PERSONALI

Io sottoscritto …… legale rappresentante dell'ente sotto identificato, pienamente informato ai sensi dell'art.13 nei limiti dell'informativa allegata, ai sensi dell'art.7 del Regolamento Europeo 2016/679:

☐ esprimo il consenso ☐ nego il consenso

Per quanto riguarda il trattamento dei nostri dati personali "particolari", nei limiti in cui sia strumentale per la finalità perseguita dall'operazione o dal servizio:

☐ esprimo il consenso ☐ nego il consenso

Per quanto riguarda la comunicazione dei dati personali a soggetti che svolgono attività funzionalmente collegate all'esecuzione dell'operazione o del servizio, quali:

- attività di elaborazione, registrazione e archiviazione dei dati, gestione della corrispondenza,
- attività bancaria e finanziaria,
- attività di trasporto e di recapito,
- altro (specificare), ……:

☐ esprimo il consenso ☐ nego il consenso

Per quanto riguarda la comunicazione dei dati personali a soggetti che svolgono attività di rilevazione della qualità dei servizi o ricerche di mercato:

☐ esprimo il consenso ☐ nego il consenso

Per quanto riguarda la comunicazione dei dati personali a soggetti che svolgono attività d'informazione commerciale:

☐ esprimo il consenso ☐ nego il consenso

Per quanto riguarda la comunicazione dei dati personali a soggetti che svolgono attività di offerta diretta di prodotti o di servizi:

☐ esprimo il consenso ☐ nego il consenso

Per quanto riguarda la possibilità di diffondere i dati personali:

☐ esprimo il consenso ☐ nego il consenso

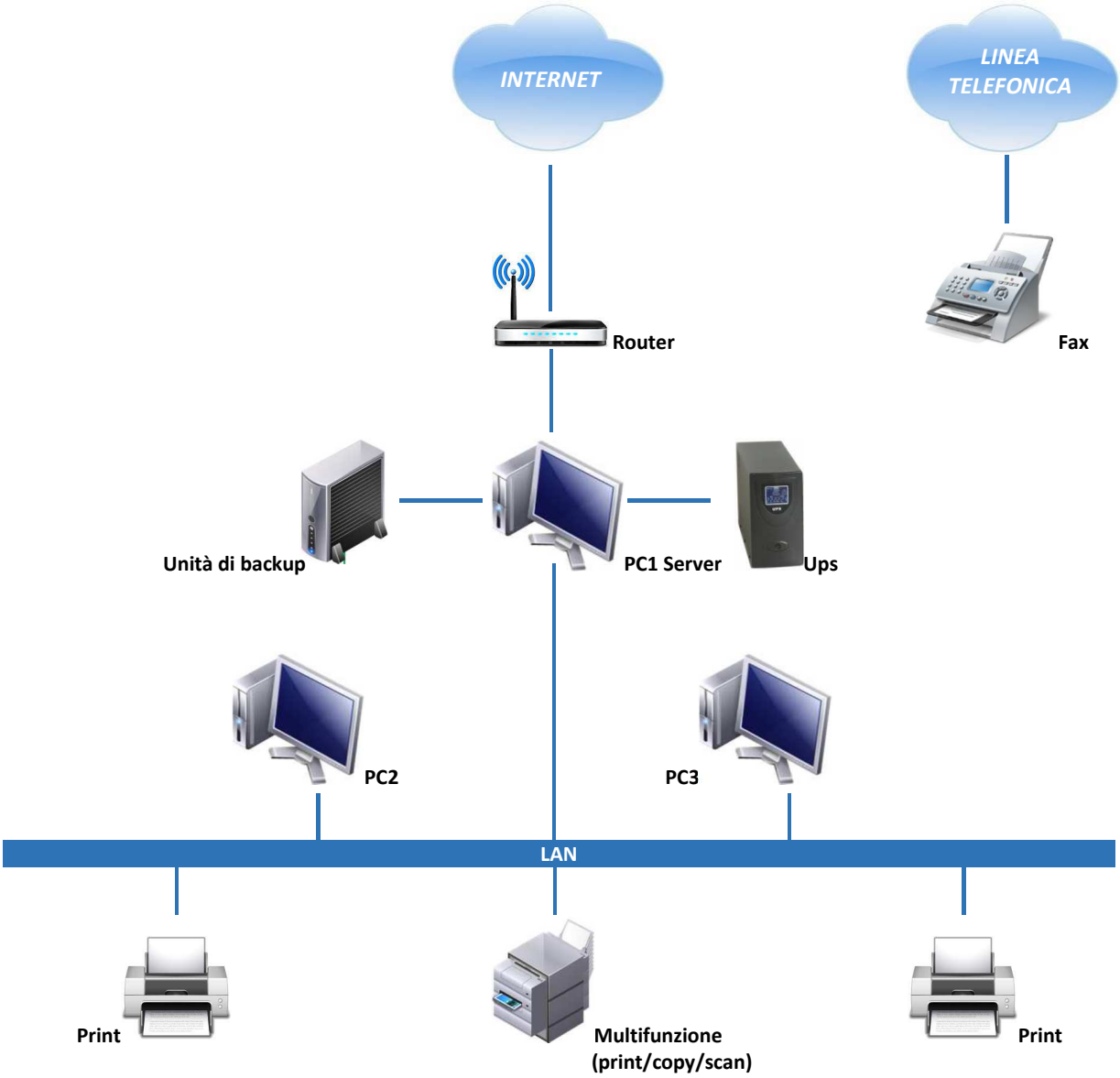
Esprimo altresì il nostro impegno a comunicarvi tempestivamente le eventuali rettifiche, variazioni e/o integrazioni dei dati in vostro possesso.

Data ..... Timbro e Firma dell'interessato ……

- Allegato 11 – Descrizione del sistema informatico dell'Ente

L'Ente è dotato del sistema informatico descritto schematicamente nella piantina sotto rappresentata ed è composto dall'hardware e dai software catalogati analiticamente nelle tabelle di seguito riportate.

Il sistema informatico accede alla rete internet tramite connessione adsl.



Periodicità delle verifiche in materia di misure minime di sicurezza

TRATTAMENTO CON L'AUSILIO DI STRUMENTI ELETTRONICI

MISURE DA VERIFICARE	DESCRIZIONE MISURA	Tipologia dei dati	CADENZA
Credenziali di autenticazione	Disattivazione in caso di mancato utilizzo dei medesimi per un periodo superiore ai 6 mesi		6 mesi
Credenziali di autenticazione	Disattivazione in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali		Sempre
Codice per l'identificazione	Una volta assegnato, non può essere assegnato ad altri incaricati		Sempre
Parola chiave	Per il trattamento di dati personali deve essere modificata ogni sei mesi		6 mesi
Parola chiave	Per il trattamento di dati particolari deve essere modificata ogni tre mesi	Dati particolari e giudiziari	3 mesi
Profili di autorizzazione	Possono essere individuati per singolo incaricato o per classi omogenee di incaricati		Sempre
Profili di autorizzazione	Verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione		1 anno
Lista degli incaricati autorizzati	Può essere redatta anche per classi omogenee di incarico		1 anno
Antivirus	Efficacia ed aggiornamento sono verificati con cadenza almeno semestrale.		6 mesi
Patch o programmi update	Programmi per elaboratore volti a correggere difetti e prevenire la vulnerabilità degli strumenti elettronici		1 anno
Patch o programmi update	Programmi per elaboratore volti a correggere difetti e prevenire la vulnerabilità degli strumenti elettronici	Dati particolari e giudiziari	6 mesi
Backup	Salvataggio dei dati con frequenza settimanale		7 giorni
RDT	Registro del Trattamento		A variazioni
Sistemi anti intrusione	Protezione contro l'accesso abusivo nel caso di trattamento di dati particolari		Sempre
Custodia dei supporti rimovibili di memorizzazione	Istruzioni organizzative e tecniche per la loro custodia e utilizzo		Sempre
Riutilizzo dei supporti di memorizzazione	Se non utilizzati devono essere distrutti o resi inutilizzabili, controllo sulla non recuperabilità delle informazioni precedentemente contenute		Sempre
Verifica dell'operato dell'Amministratore di Sistema	L'operato dell'Amministratore di Sistema è oggetto di una verifica da parte del Titolare del Trattamento Dati in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali.		1 anno

Periodicità delle verifiche in materia di misure minime di sicurezza

TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

MISURE DA VERIFICARE	DESCRIZIONE MISURA	Tipologia dei dati	CADENZA
Istruzioni scritte	Finalizzate al controllo e custodia dei documenti		Sempre
Profili di autorizzazione	Individuazione dell'ambito del trattamento consentito agli incaricati, individuati anche per classi omogenee		1 anno
Procedure di controllo e custodia	Al fine di non consentire l'accesso a persone prive di autorizzazione	Dati particolari e giudiziari	Sempre
Accesso controllato agli archivi	Le persone ammesse dopo l'orario di chiusura devono essere identificate e registrate	Dati particolari e giudiziari	Sempre
Autorizzazione preventiva all'accesso	Qualora gli archivi non siano dotati di strumenti elettronici per il controllo degli accessi o di incaricati alla vigilanza	Dati particolari e giudiziari	Sempre

Pagina destinata alla graffettatura della ricevuta dell'invio digitale