Manuale Privacy

Sistema snc

Via De Barberi n.108 - Fabbricato n.5
58100, Grosseto
C.F. / P.iva n. 01499560538

Storico delle Revisioni

Revisione	Data	Descrizione
01	**14.01.23**	**Aggiornamenti organizzativi**
00	21.08.18	Prima emissione.

Sommario

Scopo e campo di applicazione

Premessa

Dal 25 maggio 2018 si applica in Italia il Regolamento Ue in materia di protezione dei dati personali. La nuova disciplina uniforma le regole in tutti i Paesi dell'Unione e rappresenta la più grande riforma in questo settore da un quarto di secolo a questa parte.

Il Regolamento adegua il quadro normativo al nuovo contesto sociale ed economico - caratterizzato da un incessante sviluppo tecnologico e da forme sempre più massicce e pervasive di scambio e sfruttamento di dati - rafforzando le tutele poste a salvaguardia dei dati personali e i diritti degli individui.

Con il Regolamento cambia in maniera radicale l'approccio alla protezione dei dati: imprese ed enti dovranno operare seguendo il principio di responsabilizzazione ("accountability"), considerare la protezione dei dati non come obbligo formale, ma come una parte integrante e permanente delle loro attività e promuovere consapevolezza negli utenti sui loro diritti e le loro libertà.

Nello specifico, la prima novità fondamentale del Regolamento è quella di essere integralmente applicabile alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti a persone presenti nel territorio dell'Unione europea o ne monitorano il comportamento.

Tutte le aziende, ovunque stabilite, dovranno quindi rispettare le regole fissate nell'Ue.

Ogni utente avrà il diritto di ricevere informazioni chiare sull'uso che viene fatto dei suoi dati personali, potrà trasferirli da un titolare del trattamento ad un altro, compresi i social network ("diritto alla portabilità dei dati"), e vedrà rafforzato il suo diritto di far cancellare, anche on line, le informazioni non più necessarie rispetto alle finalità per le quali sono state raccolte ("diritto all'oblio").

La nuova disciplina introduce anche altre importanti misure. Imprese ed enti dovranno rispettare i principi della "privacy by design" e della "privacy by default": dovranno inserire cioè garanzie a favore degli utenti in dalla progettazione di ogni trattamento e di ogni prodotto o servizio che comporti il trattamento di dati personali. Il consenso all'uso dei dati dovrà essere ancora più specifico per ogni servizio reso. Chi tratta dati avrà l'obbligo di informare le Autorità garanti, e nei casi più gravi gli stessi interessati, in caso si verifichino furti, diffusione illecita o perdite di dati ("data breach").

Altra importante innovazione è la figura del Responsabile della protezione dei dati (RPD) che dovrà operare all'interno di tutte le amministrazioni pubbliche e di quelle imprese che fanno particolari trattamenti di dati o usano particolari categorie di dati, offrendo consulenza e supporto al proprio titolare o responsabile del trattamento.

Le sanzioni per chi non rispetta le regole potranno arrivare fino al 4 per cento del fatturato globale annuo. Tutte le Autorità di protezione dati dei Paesi Ue, alle quali è affidato il compito di vigilare sull'attuazione del Regolamento, avranno gli stessi poteri e gli stessi compiti, a garanzia ulteriore di un'applicazione realmente uniforme ed efficace nell'intera Unione.

Tale normativa integra quella nazionale oggi vigente, ovvero il Decreto legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”.

Scopo e finalità del documento

Il presente documento viene redatto, dalla Società Sistema snc (di seguito Sistema) con lo scopo di:

a) individuare tutti i processi e tutte le attività sviluppate dall’impresa che possono comportare il trattamento e la gestione di dati, classificati ai sensi della normativa applicabile;
b) valutare i rischi connessi al trattamento e alla gestione dei dati;
c) individuare le figure preposte ed i ruoli necessari al trattamento dei dati, garantendo la formazione e l’informazione delle figure di legge;
d) definire policy e procedure volte alla limitazione dei rischi di utilizzo improprio o perdita dei dati;
e) indicare le misure di prevenzione da attuate per la mitigazione dei rischi di cui alla lettera b);
f) Assicurare l’attuazione delle disposizioni di legge in materia di trattamento dei dati personali.

Definizioni

Ai sensi dell’art. 4 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, sono da considerarsi le seguenti definizioni:

«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;

«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;

«limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

«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;

«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;

«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;

«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;

«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;

«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;

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

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

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

«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;

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

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

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

«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;

«autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo

Riferimenti normativi e principi attuativi

Principi applicabili al trattamento dati personali

SISTEMA assicura che i dati personali in gestione sono:

a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Liceità del trattamento e condizioni di consenso al trattamento

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle condizioni riportate nella tabella seguente. SISTEMA, analizzato il contesto in cui opera e le attività sviluppate, ha valutato le condizioni applicabili e le relative misure di controllo necessarie, inclusi i vincoli di consenso necessari espressi dai soggetti interessati.

Qualora infatti 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.

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.

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.

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.

ID	Condizione	Applicabilità	Soggetto interessato	Consenso al trattamento
a	L'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità	**SI**	**Clienti Dipendenti**	**SI**
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	**SI**	**Clienti Dipendenti**	**SI**
c	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento	**SI**	**Dipendenti**	**SI**
d	Il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica	**NO**	**N.A.**	**N.A.**
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	**NO**	**N.A.**	**N.A.**

ID	Condizione	Applicabilità	Soggetto interessato	Consenso al 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	**SI**	**Clienti Dipendenti**	**SI**

Per quanto concerne il trattamento di dati personali di minori, SISTEMA non opera con tali dati e pertanto sono esclusi dal perimetro di applicazione del presente documento.

Trattamento di categorie particolari di dati personali

In linea con le disposizioni normative è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Tali limiti non si applicano in condizioni particolari, che SISTEMA ha valutato come di seguito illustrato.

ID	Condizione	Applicabilità	Soggetto interessato	Attività
a	L'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto	**SI**	**Dipendenti**	• **Gestione amministrativa** • **Salute sul lavoro**
b	Il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato	**NO**	**N.A.**	**N.A.**
c	Il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi	**NO**	**N.A.**	**N.A.**

ID	Condizione	Applicabilità	Soggetto interessato	Attività
	nell'incapacità fisica o giuridica di prestare il proprio consenso			
d	Il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato	**NO**	**N.A.**	**N.A.**
e	Il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato	**NO**	**N.A.**	**N.A.**
f	Il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali	**SI**	**Dipendenti**	• **Gestione amministrativa** • **Salute sul lavoro**
g	Il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato	**NO**	**N.A.**	**N.A.**
h	Il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità	**SI**	**Dipendenti**	• **Gestione amministrativa** • **Salute sul lavoro**
i	Il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del	**NO**	**N.A.**	**N.A.**

ID	Condizione	Applicabilità	Soggetto interessato	Attività
	diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale			
j	Il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1 del Regolamento europeo, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato	**NO**	**N.A.**	**N.A.**

I dati personali di cui alla lettera h), posso essere trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

SISTEMA, per il trattamento dei dati di cui alla lettere h), ha individuato la figura del Medico Competente; il soggetto è stato nominato Responsabile del Trattamento dei dati.

Trattamento dei dati personali relativi a condanne penali e reati

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1 del Regolamento europeo, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

SISTEMA può richiede, in occasione delle fasi pre-assuntive di un dipendente/collaboratore, la presentazione del casellario giudiziale e dei carichi pendenti autentificati dalle autorità pubbliche competenti; tali dati saranno gestiti in linea con prescrizioni normative vigenti.

Trattamento che non richiede l'identificazione

Se le finalità per cui un titolare del trattamento tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il presente regolamento.

Qualora, nei casi di cui sopra, il titolare del trattamento possa dimostrare di non essere in grado di identificare l'interessato, ne informa l'interessato, se possibile.

SISTEMA, effettua periodicamente un check sulle tipologie di dato trattato e, se necessario, rivaluta l'applicabilità del presente articolo, adeguando i necessari strumenti di controllo.

Diritti dell'interessato

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

Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni e le comunicazioni necessarie relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. 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.

Il titolare del trattamento agevola, nei limiti del possibile, l'esercizio dei diritti dell'interessato. Nei casi previsti dal regolamento, il titolare del trattamento non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'interessato.

Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta 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.

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.

Le informazioni fornite ed eventuali comunicazioni e azioni intraprese sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:

i. addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
ii. rifiutare di soddisfare la richiesta.

Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

Fatto salvo l'articolo 11 del Regolamento EU 2016/679, qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

Le informazioni da fornire agli interessati 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.

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

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 (non applicabile nel caso SISTEMA);
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) del Regolamento, 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.

In aggiunta alle informazioni di cui sopra, 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:

I. il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
II. 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;
III. qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a)[1], oppure sull'articolo 9, paragrafo 2, lettera a)[2] del Regolamento, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
IV. il diritto di proporre reclamo a un'autorità di controllo;
V. 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;
VI. 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.

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.

SISTEMA assicura gli adempimenti di cui sopra nei confronti di tutti i soggetti interessati.

[1] l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità

[2] l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1 del Regolamento

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

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.

Oltre alle informazioni di cui sopra, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:

I. il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
II. qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) del Regolamento, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
III. 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;
IV. qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) del Regolamento, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
V. il diritto di proporre reclamo a un'autorità di controllo;
VI. la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;

VII. l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del Regolamento, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Il titolare del trattamento fornisce le informazioni di cui ai punti precedenti:

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.

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.

I paragrafi sopra 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.

Diritto di accesso dell'interessato

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) 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.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo

spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia di cui al paragrafo precedente non deve ledere i diritti e le libertà altrui.

Diritto di rettifica

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Diritto alla cancellazione («diritto all'oblio»)

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) del Regolamento, e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1 del Regolamento, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2 del Regolamento;

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, paragrafo 1 del Regolamento.

Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo precedente, 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.

Quanto sopra riportato non si applica 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.

Diritto di limitazione di trattamento

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 del Regolamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento è limitato a norma del paragrafo 1 di cui sopra, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Diritto alla portabilità dei dati

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a) del Regolamento, o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b) del Regolamento; e

b) il trattamento sia effettuato con mezzi automatizzati.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento 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.

Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

Diritto di opposizione

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Il paragrafo 1 non si applica nel caso in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;

b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;

c) si basi sul consenso esplicito dell'interessato.

Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Ruoli e responsabilità di legge

Titolare del trattamento

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.

Se ciò è proporzionato rispetto alle attività di trattamento, le misure includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Responsabile del trattamento

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.

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.

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 del Regolamento;

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.

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.

Registri delle attività di trattamento

Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità[3]. 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

[3] L'obbligo di redazione e adozione del registro non è generale: infatti il par. 5 dell'art. 30 specifica che esso non compete "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."

i trasferimenti di cui al secondo comma dell'articolo 49 del Regolamento, 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 del Regolamento.

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 del Regolamento, 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 del Regolamento.

I registri di cui sopra sono tenuti in forma scritta, anche in formato elettronico.

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.

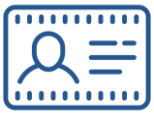
Gli obblighi di cui ai paragrafi precedenti non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di 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 del Regolamento.

SISTEMA, ancorché non obbligata, in qualità di titolare del trattamento dei dati, ha individuato le seguenti tipologie di dati e trattamenti. Per quanto concerne 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 Società ritiene non applicabile tale fattispecie di condizione.

Dati anagrafici Cliente
(nome, cognome, indirizzo, telefono, Codice Fiscale e/o Partita iva)

Tipologia di dato	Personale
Termini cancellazione	- 10 anni - A Richiesta della parte interessata
Trattamento	• Registrazione • Archiviazione informatica • Report statistici • Trasferimento per rendicontazione amministrativa
Finalità del trattamento	▪ Gestione Cliente ▪ Gestione interventi manutenzione ▪ Promozioni e marketing ▪ Gestione fatturazione
Destinatari dati	Uso interno e Società partner
Parte interessata	Cliente
Titolare trattamento	Sistema snc (Pagano, Bonucci) in caso di contatto diretto Società partner in caso di rapporto indiretto
Responsabile Trattamento	Segreteria Tecnici Commercialista
Misure di sicurezza	> Dati gestiti ai sensi di legge, informativa e consenso alla gestione > Dati gestiti su archivio informatico e cartaceo per un tempo massimo connesso alla copertura del servizio o contratto sottoscritto con fornitore elettrodomestici (garanzia e/o extra-garanzia) fino al termine del periodo di trattamento > Gestione cartacea dei dati limitato ai tempi di servizio; successiva distruzione delle copie cartacee > Archivio informativo accessibile a tecnici e segreteria, accesso a sistema informatico mediante user e password > Trasferimento dati su supporti informativi protetti



Dati amministrativi dipendente/collaboratore
(nome, cognome, indirizzo, telefono, CV, dati relativi a carichi pendenti, dati relativi a retribuzioni e/o contributi, etc.)

Tipologia di dato	Personale e giudiziario
Termini cancellazione	- 10 anni post chiusura rapporto di lavoro
Trattamento	• Registrazione • Archiviazione cartacea e informatica • Trasferimento a Commercialista per predisposizione contratto di lavoro e busta paga e atti correlati

Finalità del trattamento	▪ Costituzione rapporto lavorativo ▪ Predisposizione busta paga ▪ Adempimenti amministrativi e contributivi dipendente
Destinatari dati	Uso interno
Parte interessata	Dipendente/Collaboratore
Titolare trattamento	Sistema snc (Pagano, Bonucci)
Responsabile Trattamento	Commercialista
Misure di sicurezza	> Dati gestiti ai sensi di legge, informativa e consenso gestione rilasciato in forma scritta > Dati gestiti su archivio informatico e cartaceo per un tempo massimo di 10 anni dalla validità del documento > Trasferimento dati su supporti informativi protetti

Dati salute dipendente/collaboratore
(visite pre-assuntive, assuntive e sorveglianza sanitaria)

Tipologia di dato	Personale e sensibile
Termini cancellazione	- A chiusura del rapporto di lavoro
Trattamento	• Registrazione • Archiviazione cartacea e informatica
Finalità del trattamento	▪ Costituzione rapporto lavorativo ▪ Sorveglianza sanitaria ▪ Adempimenti di legge in materia di salute e sicurezza sui luoghi di lavoro
Destinatari dati	Uso interno
Parte interessata	Dipendente/Collaboratore
Titolare trattamento	Sistema snc (Pagano, Bonucci)
Responsabile Trattamento	Medico competente ex D.Lgs. 81/08
Misure di sicurezza	> Dati gestiti ai sensi di legge, informativa e consenso gestione rilasciato in forma scritta > Dati gestiti su archivio informatico e cartaceo fino a chiusura del rapporto di lavoro a cura del medico esterno > Conservazione su armadio chiuso a chiave presso la sede, accesso consentito al Medico

Notifica violazione dei dati

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 del Regolamento 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.

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

La notifica 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.

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.

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

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.

La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure attuate.

Non è richiesta la comunicazione all'interessato 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;

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.

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.

Processi informativi e disposizioni di sicurezza dei dati

Processi analizzati

Al fine di progettare e attuare un efficace modello di gestione delle informazioni e dei dati che garantisca il pieno rispetto della normativa sopra riportata, SISTEMA ha effettuato uno studio dei processi delle attività "core" e individuato le tipologie di dato e i principali attori interessati dalla loro gestione. Di seguito sono riportate figure e flussi di informazioni gestiti da SISTEMA.

In particolare, sono stati individuati due principali tipologie di **Soggetti interessati**:

S1: Dipendenti e collaboratori

S2: Clienti

E tre tipologie di **Responsabili trattamento dati**:

R1: Dipendenti e collaboratori

R2: Medico competente ex D.Lgs. 81/08

R3: Commercialista

Per i primi è necessario prevedere una apposita informativa, mentre per i secondi una lettera di nomina come Responsabili trattamento dati.

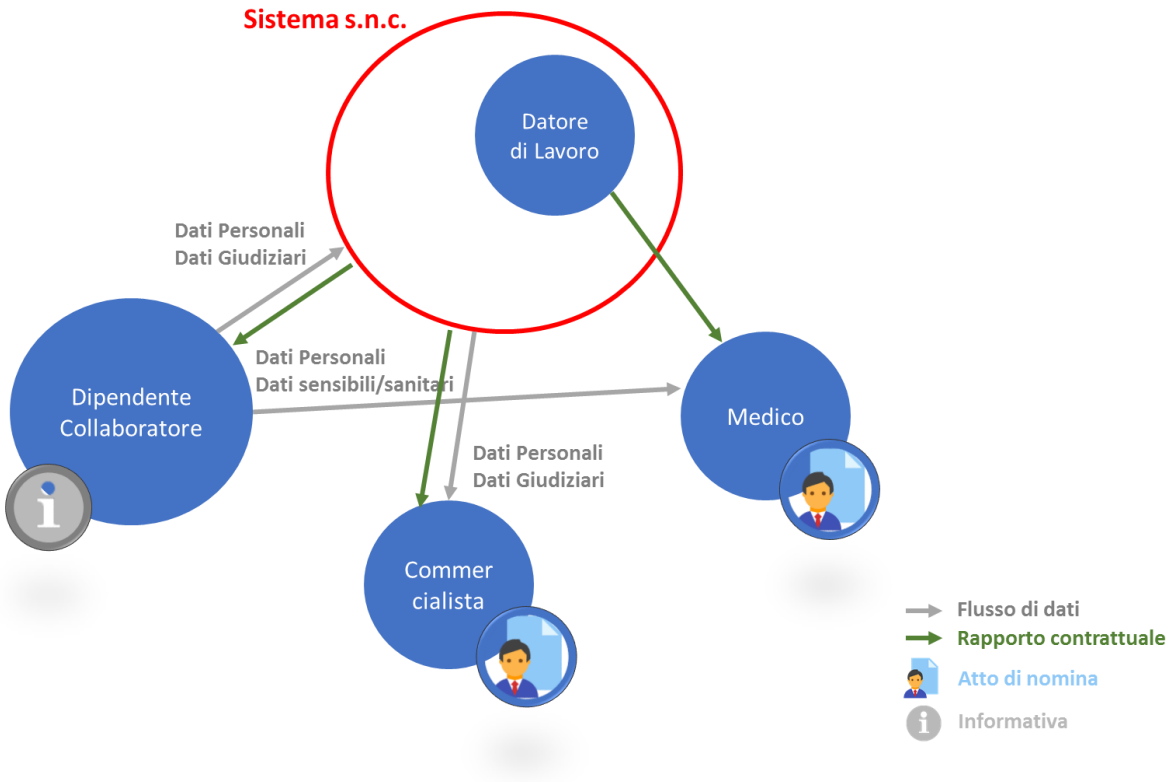


Fig.1: Rapporti informativi e contrattuali Dipendenti e Collaboratori

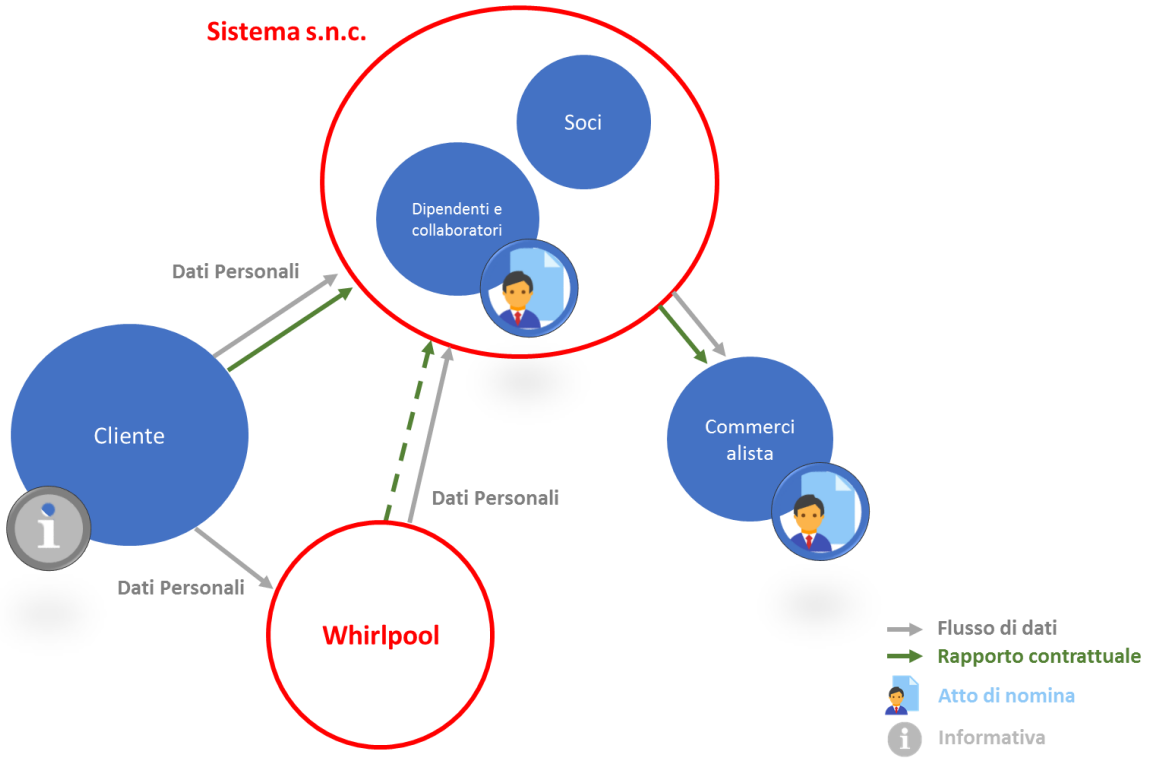


Fig.2: Rapporti informativi e contrattuali Clienti

Informativa e consenso per i dipendenti/collaboratori - strumenti

I dipendenti ed i collaboratori in fase pre-assuntiva sottopongono i propri CV, mediante posta elettronica o consegna a mano di copia cartacea, a SISTEMA corredata da apposita dichiarazione al trattamento dei dati.

Prima della stipula del contratto, SISTEMA fornisce idonea informativa sulle attività di trattamento dei dati ai propri dipendenti e acquisisce formale consenso al trattamento da parte di quest'ultimi.

Al termine del rapporto contrattuale, SISTEMA assicura la restituzione e, se necessario, la distruzione dei dati gestiti.

Informativa e consenso per i clienti - strumenti

I clienti possono entrare in contatto con SISTEMA secondo diverse modalità, di seguito un prospetto che rappresenta tali modalità e le tecniche di informativa e acquisizione del consenso al trattamento dei dati.

TIPOLOGIA	MODALITÀ	DETTAGLI OPERATIVI
Contatto diretto SISTEMA-CLIENTE	Sito Internet	Nel proprio sito internet SISTEMA ha riportato idonee informative circa le policy di privacy attuate dalla società relativamente alle modalità di gestione del Sito (e dei relativi cookie) e alle modalità di gestione dei dati relativamente alle assistenze tecniche in favore dei propri clienti
	Pagina Facebook	SISTEMA risponde alle richieste di informazioni dei propri Clienti senza mantenere registrazione dei relativi dati generali. Per quanto riguarda la prenotazione di interventi e quindi l'attivazione dei servizi di SISTEMA, queste sono centralizzate sui linee telefoniche dedicate
	Posta elettronica / PEC	
	Telefono	SISTEMA durante la fase iniziale di contatto con il Cliente fornisce una informativa di sintesi sulle modalità di trattamento dei dati e rimanda al sito internet per ulteriori approfondimenti
	Rapporto frontale col Cliente	SISTEMA, alla prima occasione di contatto diretto con il Cliente, illustra (o rammenta) a quest'ultimo l'informativa sulla privacy e ne acquisisce l'autorizzazione al trattamento
Contatto indiretto SISTEMA-CLIENTE	Ticket centro coordinamento intervento esterno	SISTEMA è stata preventivamente incaricata della gestione dei dati dei Clienti dai propri partner; nell'area informativa del proprio sito internet, SISTEMA descrive tale fattispecie rimandando, ove necessario, alle policy privacy delle società produttrici degli elettrodomestici
	Rapporto frontale col Cliente	SISTEMA, alla prima occasione di contatto diretto con il Cliente, illustra (o rammenta) a quest'ultimo l'informativa sulla privacy e ne acquisisce l'autorizzazione al trattamento

Misure di protezione su documenti cartacei

Il trattamento di dati personali effettuato su supporti cartacei è consentito nel rispetto delle seguenti misure minime di sicurezza:

a. I documenti/dati devono essere conservati in appositi armadi custoditi e inaccessibili a personale non preventivamente autorizzato dal Titolare del trattamento dei dati;
b. La copia dei documenti è consentita per le finalità individuate dal Titolare del trattamento dei dati; rilasci di informazioni non controllate saranno tempestivamente segnalate e saranno previste idonei strumenti di controllo;
c. Una volta completato il ciclo di utilizzo delle informazioni su supporto cartacee queste saranno distrutte mediante apposito trita-carte.

Misure di protezione su documenti informatizzati

Il trattamento di dati personali effettuato con strumenti elettronici è consentito nel rispetto delle seguenti misure minime di sicurezza:

a. *autenticazione informatica*: i soggetti autorizzati al trattamento dei dati sono profilati, l'accesso ai sistemi è consentito mediante username e password;
b. *adozione di procedure di gestione delle credenziali di autenticazione*: le credenziali di accesso sono assegnate dall'amministratore di sistema su richiesta del Titolare trattamento dati;
c. *utilizzazione di un sistema di autorizzazione*: che prevede accessi in funzione delle attività;
d. *aggiornamento periodico e manutenzione degli strumenti elettronici*: dotati di strumenti di riconoscimento e protezione dai virus informatici;
e. *protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici*: attuato mediante appositi tool;
f. *adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi*: garantito mediante back up periodico dei dischi di sistema.