

	<i>Systems Projects Services srl</i>	ITC-154596	
	Regolamento privacy e trattamento dati personali SPS	Sh. 1 of 22	Rev.0

Regolamento privacy e trattamento dati personali SPS



INDICE

1. GENERALE	3
2. TITOLARE	4
3. DEFINIZIONI	5
4. TRATTAMENTO	7
4.1. "Persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (Rif. Art. 4, n. 10, del Regolamento)	7
5. INFORMAZIONE AGLI INTERESSATI (INFORMATIVA)	8
5.1. Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato	8
5.2. Informazioni da fornire qualora i dati personali non siano raccolti presso l'interessato	8
6. DIRITTI DELL'INTERESSATO	10
7. DISPOSIZIONI GENERALI	15
7.1. Trattamento dei dati senza l'ausilio di supporti elettronici	15
7.2. Utilizzo degli strumenti informatici	15
7.3. Sistema elettrico e sistema informatico	16
7.4. Rete Internet	17
7.5. Casella di posta elettronica	18
7.6. Gestione dell'account di posta elettronica successivamente alla cessazione del rapporto di lavoro e/o collaborazione	19
7.7. Accesso alla posta elettronica nell'ambito del programma BYOD	19
7.8. Utilizzo del Personal Computer (PC)	19
7.9. Dispositivi mobili	20
7.10. Utilizzo dei dispositivi personali per fini lavorativi (BYOD)	20
7.11. Controllo sul rispetto delle modalità di utilizzo di Internet e della posta elettronica	21
7.11.1. Controllo ordinario	21
7.11.2. Controllo straordinario	22

	Systems Projects Services srl Regolamento privacy e trattamento dati personali SPS	ITC-154596	
		Sh. 3 of 22	Rev.0

1. GENERALE

Al fine di garantire all'interno della Systems Projects Services Srl puntuale applicazione della normativa vigente in fatto di protezione di dati personali e del nuovo Regolamento 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, la Direzione emana il seguente Regolamento Aziendale.

Il presente Regolamento Aziendale, il cui rispetto è obbligatorio per tutti i collaboratori dell'azienda, ha lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone, così come specificato dalla vigente normativa.

Il presente regolamento può essere di volta in volta integrato in base a nuove/diverse disposizioni dettate dai clienti, dall'entrata in vigore di nuove disposizioni, da implementazioni che l'Azienda vorrà apportare.

	Systems Projects Services srl Regolamento privacy e trattamento dati personali SPS	ITC-154596	
		Sh. 4 of 22	Rev.0

2. TITOLARE

Il titolare del trattamento dei dati è la Systems Projects Services Srl, qui di seguito denominata Azienda. Il titolare del trattamento, quale responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa decide il motivo e le modalità del trattamento e pone in essere misure tecniche e organizzative adeguate per garantire la tutela dei diritti dell'interessato.

	Systems Projects Services srl	ITC-154596	
	Regolamento privacy e trattamento dati personali SPS	Sh. 5 of 22	Rev.0

3. DEFINIZIONI

Di seguito si riportano, per praticità, alcune definizioni tratte dal Regolamento Europeo.

Ai fini del presente regolamento s'intende per:

- *«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;*
- *«collaboratore»: la persona fisica che svolge le proprie mansioni per conto di Systems Projects Services Srl come lavoratore dipendente, come libero professionista o come dipendente di Terzi;*
- *«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*

	Systems Projects Services srl	ITC-154596	
	Regolamento privacy e trattamento dati personali SPS	Sh. 6 of 22	Rev.0

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.*

	Systems Projects Services srl Regolamento privacy e trattamento dati personali SPS	ITC-154596	
		Sh. 7 of 22	Rev.0

4. TRATTAMENTO

Qualunque trattamento dei dati personali posto in essere dall'Azienda è consentito, fatto salvo il rispetto dei presupposti e dei limiti stabiliti dal Regolamento e dalle norme vigenti, anche in relazione alla diversa natura dei dati, soltanto per lo svolgimento delle funzioni di propria competenza. I dati personali devono essere trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e devono anche essere esatti, aggiornati, pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti e trattati. Nel trattamento è autorizzata solo l'esecuzione delle operazioni strettamente necessarie al perseguimento delle finalità per le quali lo stesso è stato consentito, anche quando i dati sono raccolti nello svolgimento di attività di vigilanza, ispettive o di controllo. Il trattamento dei dati particolari è invece consentito solo se autorizzato da espressa disposizione di legge, obblighi contrattuali, esplicito e preventivo consenso, legittimo interesse del Titolare del Trattamento.

4.1. "Persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (Rif. Art. 4, n. 10, del Regolamento)

Le persone autorizzate al trattamento sono individuati dal Titolare, con apposito atto scritto nel quale debbono essere espressamente precisati gli "ambiti" del trattamento consentito. A prescindere, comunque, dalla formale attribuzione della qualifica di persona autorizzata, i collaboratori dell'Azienda, nonché tutti coloro che vi operano, a qualsiasi titolo, con o senza retribuzione, gli specializzandi, i tirocinanti ed i volontari, sono tenuti al rispetto di quanto previsto dal presente regolamento e dalla normativa vigente, qualora durante la loro attività vengano a conoscenza di dati personali.

Tutti i soggetti di cui sopra, in particolare, sono tenuti a:

- a) osservare tutte le istruzioni in ordine al trattamento dei dati personali ed ai connessi profili della sicurezza;
- b) astenersi da qualunque comportamento o operazione che non sia coerente con l'espletamento dei propri compiti istituzionali;
- c) impegnarsi a non comunicare e diffondere all'esterno dell'Azienda, per finalità diverse da quelle del rapporto di lavoro, i dati personali di cui siano venuti comunque a conoscenza nell'ambito della propria attività;
- d) rispettare in maniera precisa le indicazioni che, in caso di assegnazione temporanea di luogo di lavoro presso un' Azienda cliente, quest'ultima avrà impartito, ponendo cura e massima attenzione laddove si rivelino mancanze di regolamenti/mansionari/procedure, di adottare in ogni caso tutte le misure obbligatorie e idonee a salvaguardare le informazioni di cui si verrà a conoscenza, integrando le buone prassi di comportamento alle disposizioni del regolamento Systems Projects Services Srl e alle misure di sicurezza così come previste dalla normativa vigente.

Le nomine delle persone autorizzate, firmate per accettazione, sono conservate dal Titolare del Trattamento. Periodicamente, con cadenza almeno annuale, il Titolare, tramite anche persone a questo demandate, procede ad aggiornare la definizione dei dati cui gli Incaricati sono autorizzati ad accedere e verifica i requisiti dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

	Systems Projects Services srl	ITC-154596	
	Regolamento privacy e trattamento dati personali SPS	Sh. 8 of 22	Rev.0

5. INFORMAZIONE AGLI INTERESSATI (INFORMATIVA)

Il collaboratore/dipendente che per motivi lavorativi si trovi nella condizione di trattare dati personali di terzi, dovrà accertarsi, a ogni nuovo trattamento e preventivamente, che questi abbiano tutte le informazioni relative al trattamento dei propri dati, con un linguaggio semplice e chiaro, per iscritto o con altri mezzi, anche elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Le informazioni possono essere rilasciate in maniera orale o scritta (Documento Informativa) facendo attenzione a che siano esplicite alcuni dati, riportati nei paragrafi successivi.

L'informativa (Art. 13 del Codice, Artt. 13 e 14 del Regolamento) deve essere sempre fornita all'interessato, intesa come persona fisica, prima di effettuare la raccolta dei dati. Se i dati non sono raccolti direttamente presso la persona interessata, l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento. In tutti i casi, è obbligo specificare l'identità del Titolare le finalità del trattamento, i diritti degli interessati (compreso il diritto alla portabilità dei dati), e quali sono i destinatari dei dati. Nel caso di dati personali non raccolti direttamente presso l'interessato, l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (dei dati (a terzi o all'interessato)). L'informativa può anche essere esposta in sintesi purché ci sia una copia integrale della stessa disponibile presso la sede del Titolare del Trattamento e/o nel sito internet.

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

In caso di raccolta presso l'interessato di dati che lo riguardano, l'interessato è tenuto a ricevere alcune informazioni tra cui l'identità e i dati di contatto del titolare del trattamento, le finalità e la base giuridica, gli eventuali legittimi interessi perseguiti dal Titolare del Trattamento o da terzi, gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e, ove applicabile, l'intenzione 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, l'interessato ha diritto a ricevere informazioni necessarie per garantire un trattamento corretto e trasparente come il periodo di conservazione dei dati personali, i suoi diritti (di cui al paragrafo successivo), l'esistenza di un processo decisionale automatizzato, compresa la profilazione (Art. 22, paragrafi 1 e 4) e 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 è necessario fornire all'interessato informazioni in merito.

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

Qualora i dati non siano stati ottenuti presso l'interessato, lo stesso è tenuto a sapere la fonte da cui hanno origine i dati personali. Le informazioni dovranno essere comunicate entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un

	<i>Systems Projects Services srl</i> Regolamento privacy e trattamento dati personali SPS	ITC-154596	
		Sh. 9 of 22	Rev.0

mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati. Va inoltre preventivamente specificata la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

	Systems Projects Services srl Regolamento privacy e trattamento dati personali SPS	ITC-154596	
		Sh. 10 of 22	Rev.0

6. DIRITTI DELL'INTERESSATO

Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato 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.

Diritto di accesso dell'interessato (Art. 15)

1. 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.
2. 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.
3. 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.
4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

Diritto di rettifica (Art. 16)

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») (Art. 17)

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, paragrafo 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;
 - e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Diritto di limitazione di trattamento (Art. 18)

1. 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, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.
2. Se il trattamento è limitato a norma del paragrafo 1, 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

	Systems Projects Services srl Regolamento privacy e trattamento dati personali SPS	ITC-154596	
		Sh. 12 of 22	Rev.0

tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

3. 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 (Art. 19)

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 (Art. 20)

1. 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), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b);
 - b) il trattamento sia effettuato con mezzi automatizzati.
2. 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.
3. 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.
4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

Sezione 4

Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche

Diritto di opposizione (Art. 21)

1. 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.
2. 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.



3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.
4. 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.
5. 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.
6. 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 (Art. 22)

1. 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.
2. 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.
3. 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.
4. 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.

Comunicazione di una violazione dei dati personali all'interessato (Art. 34)

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;

	Systems Projects Services srl	ITC-154596	
	Regolamento privacy e trattamento dati personali SPS	Sh. 14 of 22	Rev.0

- b) 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;
 - c) 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;
 - d) 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.

	Systems Projects Services srl Regolamento privacy e trattamento dati personali SPS	ITC-154596	
		Sh. 15 of 22	Rev.0

7. DISPOSIZIONI GENERALI

Presso Systems Projects Services Srl vengono eseguiti i trattamenti in maniera conforme a quanto previsto dalla disciplina vigente. A tal fine mette in atto misure di sicurezza tali da garantire l'integrità, la disponibilità e la riservatezza dei dati trattati, sia in termini di allocazione delle risorse umane e delle risorse tecnologiche, sia in termini normativi e comportamentali in funzione di una maggior "responsabilizzazione" (accountability) nei confronti della materia.

Systems Projects Services Srl ponendo grande attenzione agli aspetti della sicurezza individua, definisce e assegna formalmente i ruoli e le responsabilità inerenti il trattamento delle informazioni dei dati. L'azienda ricorda che nell'esecuzione delle proprie mansioni l'incaricato potrà venire a conoscenza di informazioni riservate, sia di tipo commerciale/finanziario, che di dati personali riferibili a terzi. I dati suddetti, oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite, in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento, in modo tale da ridurre al minimo, mediante l'adozione di idonee misure di sicurezza, i rischi di distribuzione o di perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito e non conforme alle finalità di raccolta.

Il trattamento è limitato a quei dati strettamente necessari agli adempimenti contrattuali. Rimangono vietate operazioni e trattamenti di qualunque genere che vadano oltre gli scopi del contratto e delle proprie mansioni. La comunicazione e la diffusione sono proibite. E' fatta salva, comunque, la comunicazione o la diffusione dei dati, in conformità alla legge, su richieste effettuate da forze di polizia, autorità giudiziaria, organismi di informazione e sicurezza o da altri soggetti pubblici, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

7.1. Trattamento dei dati senza l'ausilio di supporti elettronici

La documentazione cartacea all'interno dell'ufficio deve essere sempre risposta in mobili, cassettiere e armadi, chiusi a chiave, non accessibili da personale non autorizzato. Per custodire qualsiasi tipo di documento, soprattutto in circostanze in cui gli stessi devono essere portati fuori dai locali, non si fa uso di cartelle trasparenti, a meno che non siano contenute all'interno di appositi raccoglitori coprenti. Appunti, informazioni, note, non vanno lasciate in giro all'interno dei locali o trascritti in supporti che possono essere visti. La carta da gettare è distrutta tramite distruggi documenti che è posizionata all'interno della sede. La carta che non contiene informazioni personali come dispense di studio, pubblicità, ecc., viene gettata nel raccoglitore per la raccolta differenziata adibito. Non è consentito in alcun caso utilizzare carta riciclata per la stampa o per qualsiasi altro utilizzo.

7.2. Utilizzo degli strumenti informatici

Le disposizioni di legge principali e i documenti concernenti la corretta gestione di sistemi informatici sono:

- R.D. 22.4.1941 n. 633 e D.Lgs. 29.12.1992 n. 518 (tutela del diritto di autore sul software);
- L. 23.12.1993 n. 547 (reati legati all'informatica - modifiche al Codice penale);
- D.lgs.vo 30.6.2003 n.196 (recante il Codice in materia di protezione dei dati personali) e suo Disciplinare Tecnico (Allegato B);
- Lavoro: le linee guida del Garante per posta elettronica e internet Gazzetta Ufficiale n. 58 del 10 marzo 2007;

	Systems Projects Services srl Regolamento privacy e trattamento dati personali SPS	ITC-154596	
		Sh. 16 of 22	Rev.0

- Reti telematiche ed Internet - L'indirizzo e-mail è un dato personale Provvedimento (22 giugno 2002);
- Regolamento Europeo 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- Cloud computing: indicazioni per l'utilizzo consapevole dei servizi Norme di utilizzo;
- La reputazione online tra principi di dignità e diritto all'oblio digitale Intervento di Antonello Soro, Presidente del Garante per la protezione dei dati personali ("L'Huffington Post", 6 ottobre 2015);
- Accesso alla posta elettronica dei dipendenti - 22 dicembre 2016.

7.3. Sistema elettrico e sistema informatico

L'accesso al sistema aziendale da parte dei collaboratori, o chiunque per finalità esplicite e precise si trovi a utilizzarlo, dovrà avvenire in conformità a quanto previsto dal presente regolamento e/o in conformità al regolamento alla quale il sistema fa riferimento. Si precisa che l'accesso e l'utilizzo sono consentiti ai soli fini dell'esecuzione della prestazione per la quale l'utente è stato abilitato.

Al fine di salvaguardare il corretto funzionamento della rete elettrica e della rete internet e tutte le impostazioni a esse connesse, si fa presente che non è consentito:

- accedere a linee informatiche non consentite e non specificate nelle proprie lettere di incarico e/o accedere a linee non conosciute con gli strumenti di lavoro;
- accedere ai quadri elettrici e/o modem, né modificare alcun settaggio dell'impiantistica installata nell'area di lavoro;
- eseguire nuovi allacciamenti elettrici/fonia/dati;
- utilizzare apparecchiature che possano causare particolari picchi o abbassamenti di tensione o compiere attività che possano creare particolari rischi di incendio od esalazioni tossiche;
- utilizzare cavi, prolunghe, connettori, ecc., non certificate alle norme vigenti e non autorizzate dall'Azienda;
- utilizzare, anche in sola ricezione, walkie-talkie o apparecchiature di rice-trasmissione non autorizzate dall'Azienda;
- utilizzare dispositivi e apparati di trattamento dei dati quali ad esempio PC, work station, dispositivi di memorizzazione, ecc., che non siano autorizzati dall'Azienda o che, anche se autorizzati, non rispondano ai requisiti di sicurezza stabiliti dalla legislazione in merito;
- connettere dispositivi e apparati di trattamento dei quali ad esempio PC, work station, dispositivi di memorizzazione, ecc., alle reti aziendali senza espressa autorizzazione dall'Azienda;
- utilizzare, per mansioni legate allo sviluppo, esercizio o manutenzione di prodotti, dati e informazioni, non autorizzati dalla società;
- trattare informazioni e dati al di fuori di quanto espressamente previsto dal proprio mansionario;
- eseguire installazioni, alterazioni (inclusa installazione di software di qualsiasi genere, licenziato e non licenziato) e modifiche, dismissioni di materiale e/o componenti hardware e software, e supporti di memorizzazione di qualsiasi tipo;
- utilizzare supporti di memorizzazione removibile non autorizzati su infrastrutture e sistemi di proprietà della società;
- installare infrastrutture di networking, comunicazione o connettività, di tipo locale o remoto, fatto salvo esigenze derivanti da obblighi contrattuali preventivamente ed esplicitamente previste;

	Systems Projects Services srl Regolamento privacy e trattamento dati personali SPS	ITC-154596	
		Sh. 17 of 22	Rev.0

- utilizzo di strumenti preposti alla scansione ed alla rilevazione delle vulnerabilità di sistemi, applicazioni e servizi, così come di soluzioni hardware e software identificate, considerate o riconosciute come strumenti di hacking, cracking o diffusione di virus e spam.

7.4. Rete Internet

L'accesso alla rete internet è consentita tramite apposita password fornita dal Titolare del Trattamento o da un suo delegato. Si potrà accedere, nel caso di più reti, solo alla rete assegnata.

Il PC e comunque ogni strumento abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. È per questo vietato compiere attività che appesantiscano il traffico o i servizi sulla rete, come pure compiere attività che possano causare disturbi al sistema senza valutarne adeguatamente le conseguenze. E' altresì assolutamente proibita con gli strumenti di lavoro la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

Si ricorda inoltre che in relazione agli strumenti di lavoro aziendali e per uso lavorativo aziendale:

- E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati) e di bacheche elettroniche, nonché la registrazione in guest books anche utilizzando pseudonimi (o nicknames). Il Titolare del Trattamento si riserva di individuare i siti considerati correlati con la prestazione lavorativa e di inserire eventuali filtri che prevengano determinate operazioni (quali l'accesso a siti inseriti in una sorta di black-list o il download di file musicali o multimediali).
- Accedere a siti dal contenuto non attinente allo svolgimento dell'attività lavorativa e in tutti i casi in cui la navigazione sia idonea a rivelare dati sensibili ai sensi del Codice Privacy.
- Accedere a siti internet evitando l'azione o comunque superando o tentando di superare o disabilitando i sistemi adottati dalla Società per bloccare l'accesso ad alcuni siti ed in ogni caso utilizzare siti o altri strumenti (es. Cracking Programs) che realizzino tale fine.
- Effettuare il download di software gratuito (freeware) o messo a disposizione in rete per essere provato (shareware, demo), e comunque il download di qualsiasi software senza l'espressa autorizzazione del Titolare del Trattamento.
- Accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
- Promuovere utile o guadagno personale.
- Utilizzare internet in violazione delle norme in vigore dell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248).

Dal momento che la violazione delle summenzionate regole potrebbe esporre la società al rischio di danneggiamento o mal funzionamento del sistema informatico, il rispetto di tali regole potrà essere oggetto di controllo anche mediante accesso in remoto, attraverso periodiche verifiche del contenuto della memoria di massa del server e del PC consegnato al collaboratore (si vedano i paragrafi 3.1 e 3.2 della presente procedura).

	Systems Projects Services srl Regolamento privacy e trattamento dati personali SPS	ITC-154596	
		Sh. 18 of 22	Rev.0

7.5. Casella di posta elettronica

La casella di posta elettronica assegnata al collaboratore è uno strumento di lavoro e verrà usato per l'invio delle comunicazioni relative alla sua mansione per questa azienda. Come persona assegnataria della suddetta casella di posta l'utente sarà responsabile del corretto utilizzo della stessa.

A tal fine si precisa che:

- È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list, o per qualsiasi altra funzione diversa da quella esplicitamente autorizzata.
- L'iscrizione a mailing list esterne è concessa solo per motivi professionali: prima di iscriversi occorre verificare in anticipo se il sito è affidabile.
- Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli. Nel caso di messaggi provenienti da mittenti sconosciuti ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti.
- Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (zip, rar, jpg).
- Nel caso in cui si debba inviare un documento all'esterno è preferibile utilizzare un formato protetto da scrittura e modifiche (ad esempio il formato Acrobat pdf).
- La casella di posta deve essere mantenuta in ordine cancellando documenti inutili e soprattutto allegati ingombranti. È obbligatorio controllare gli allegati di posta elettronica prima del loro utilizzo (la provenienza deve essere attendibile e il tipo di file sicuro).
- Potrebbero venir resi disponibili anche indirizzi condivisi tra più lavoratori, rendendo così chiara la natura non privata della corrispondenza.
- Sono poi previsti, in caso di assenza del lavoratore, messaggi di risposta automatica con le coordinate di altri lavoratori cui rivolgersi. Il datore mette infine il collaboratore in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al titolare quelli ritenuti rilevanti per l'ufficio in caso di assenza prolungata o non prevista e di improrogabili necessità legate all'attività lavorativa.
- La mail aziendale dovrà riportare la firma corretta, con i dati del lavoratore, compresa la sua mansione, e dell'azienda così come disposto dalla direzione. La firma dovrà sempre avere il disclaimer della privacy, impostata di default al momento dell'impostazione dell'account.
- Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per Systems Projects Services Srl deve essere visionata od autorizzata dalla Direzione o da un Responsabile se non si ha ricevuto preventivamente una opportuna delega. La documentazione elettronica che costituisce per l'azienda "know-how" aziendale tecnico o commerciale protetto, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione. Per le comunicazioni ufficiali è possibile avvalersi posta tradizionale o della posta certificata seguendo le disposizioni contenute nel Regolamento Interno.

	Systems Projects Services srl Regolamento privacy e trattamento dati personali SPS	ITC-154596	
		Sh. 19 of 22	Rev.0

7.6. Gestione dell'account di posta elettronica successivamente alla cessazione del rapporto di lavoro e/o collaborazione

Successivamente alla cessazione del rapporto di lavoro e/o collaborazione la casella di posta elettronica sarà disattivata. Sarà inoltre predisposto temporaneamente un sistema di risposta automatica per informare il mittente dell'avvenuta disattivazione dell'account di posta elettronica e dare indicazione del nuovo referente aziendale se necessario. Il contenuto degli account di posta elettronica disattivati sarà registrato in un file di backup. Successivamente alla cessazione del rapporto di lavoro e/o collaborazione, la Società potrà liberamente accedere al contenuto del file di backup, del personal computer nonché alla casella di posta elettronica assegnata al lavoratore durante il rapporto di lavoro nel caso di ragionevoli motivi come quelli di continuità dell'attività della Società, per finalità di sicurezza del sistema informatico, nonché quando ciò sia necessario.

7.7. Accesso alla posta elettronica nell'ambito del programma BYOD

Le regole stabilite nel presente documento della presente procedura sono applicabili, in relazione alle sole applicazioni aziendali, anche per l'utilizzo della posta elettronica nell'ambito del programma BYOD.

7.8. Utilizzo del Personal Computer (PC)

Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire a innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. L'accesso al computer è protetto da credenziali univoche e personali. È specificato che l'utente è responsabile per il proprio computer e per l'uso che ne viene fatto.

Solo il Titolare del Trattamento, o persona autorizzata (interna o esterna a SPS purché formalmente incaricata) per l'espletamento delle sue funzioni, ha la facoltà di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato e nel caso non sia stato nominato un sostituto a questa funzione, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Si ribadisce altresì che:

- Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del Titolare del Trattamento, in quanto sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni del computer.
- Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal responsabile dei sistemi informatici e autorizzati dal Titolare del Trattamento. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

	Systems Projects Services srl Regolamento privacy e trattamento dati personali SPS	ITC-154596	
		Sh. 20 of 22	Rev.0

- Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita del Titolare del Trattamento.
- Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ...), se non con l'autorizzazione espressa del Titolare del Trattamento.
- Il PC non deve mai essere lasciato incustodito connesso alla rete in quanto può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso l'accesso alla postazione di lavoro deve essere bloccato ogni qual volta ci si allontani da essa (digitando sulla tastiera "CTRL+ALT+CANC")
- Sui computer dotati di scheda audio e/o di lettore cd non è consentito l'ascolto di programmi, file audio o musicali, se non a fini prettamente lavorativi.
- Il PC deve essere sempre mantenuto in posizione idonea e sicura affinché si evitino cadute e rotture dovute a urti accidentali.
- Il Pc va mantenuto pulito e nella massima efficienza. E' cura dell'incaricato a cui lo stesso è affidato provvedere alla pulizia dei file e del materiale non più necessario in modo da mantenere il PC perfettamente operativo.
- In caso di malfunzionamento, manutenzione straordinaria, incidente, o problemi che si possano riscontrare nel PC, l'incaricato dovrà confrontarsi con il Titolare del Trattamento e non intervenire in modo autonomo.

7.9. Dispositivi mobili

L'utente è responsabile dei dispositivi mobili assegnatogli e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo, nel luogo di lavoro come fuori dagli stessi. Ai dispositivi mobili si applicano le regole di utilizzo previste per materiali connessi in rete con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

- I dispositivi mobili utilizzati all'esterno in caso di allontanamento, devono essere custoditi in un luogo protetto. Questi non devono essere mai lasciati incustoditi e sul disco devono essere conservati solo i file strettamente necessari.
- Nel caso di accesso alla rete tramite RAS (Remote Access Server) / Accesso Remoto utilizzare l'accesso in forma esclusivamente personale ed utilizzare la password in modo rigoroso.
- Disconnettersi dal sistema RAS al termine di ogni sessione di lavoro. Collegarsi periodicamente alla rete per consentire il caricamento dell'aggiornamento dell'antivirus.
- In caso di furto o smarrimento di strumenti informatici della Systems Projects Services Srl, il collaboratore al quale gli stessi strumenti sono affidati, oltre che denunciare l'accaduto all'Autorità, deve tempestivamente darne comunicazione al Titolare del Trattamento.
- Proteggere i dispositivi mobili da accessi non autorizzati o da infezione da codice malevolo.

7.10. Utilizzo dei dispositivi personali per fini lavorativi (BYOD)

E' opportuno precisare che, qualora sul dispositivo di uso "ibrido" siano presenti dati o informazioni aziendali qualificabili come personali, per i quali la Società riveste il ruolo di Titolare del trattamento in virtù della normativa vigente, vige l'obbligo di porre in essere gli adempimenti previsti dai Regolamenti Aziendali dal Regolamento Europeo e dai Provvedimenti dall'Autorità Garante.

	Systems Projects Services srl Regolamento privacy e trattamento dati personali SPS	ITC-154596	
		Sh. 21 of 22	Rev.0

7.11. Controllo sul rispetto delle modalità di utilizzo di Internet e della posta elettronica

La Società promuove ogni opportuna misura organizzativa, tecnologica e di sicurezza volta a prevenire il rischio di utilizzi indebiti che possano ingenerare responsabilità di natura civile o penale oltre a "minimizzare" l'uso di dati riferibili ai lavoratori e collaboratori e a garantire la disponibilità e l'integrità dei sistemi informativi e dei dati; allo scopo, la Società ha adottato strumenti tecnici e organizzativi volti a prevenire trattamenti illeciti sui dati trattati con strumenti informatici, come illustrato nei regolamenti aziendali. La Società informa di aver adottato sistemi che evitino interferenze ingiustificate sui diritti e sulle libertà fondamentali dei lavoratori/collaboratori e dei soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata, nel rispetto del principio di pertinenza e non eccedenza, con esclusione di qualunque registrazione o monitoraggio sistematico e di analisi occulta. Premesso che l'uso del PC aziendale, di internet e dell'indirizzo di posta elettronica aziendale, attraverso le apparecchiature aziendali, è consentito solo per motivi di lavoro e nell'interesse esclusivo della Società, mentre ne è vietato l'uso personale, e che l'utilizzo dei sistemi informatici non conforme alle regole di cui alla presente Policy può comportare delle serie minacce alla sicurezza informatica e alla corretta conservazione dei dati essenziali per l'attività della Società nonché il rischio di sanzioni civili, amministrative e penali sia per la Società sia per lo stesso lavoratore, la Società si riserva espressamente il diritto di esercitare controlli (ad esempio per fini di manutenzione, per esigenze di sicurezza, e/o per verificare il rispetto delle modalità di utilizzo da parte dei collaboratori degli strumenti informatici in dotazione, nonché al fine di prevenire e/o accertare la commissione di atti che possono costituire reati o comunque atti illeciti). I controlli possono avvenire secondo due livelli, denominati rispettivamente "ordinario" e "straordinario", secondo le modalità di seguito descritte.

7.11.1. Controllo ordinario

Il primo livello di controllo "ordinario" viene svolto in maniera anonima e in caso di elusione dei filtri preventivi preimpostati che riducono al minimo l'esigenza del controllo successivo. Il sistema di Firewall per l'accesso a siti Internet di contenuto illecito o comunque non attinente all'attività lavorativa nonché il sistema di filtraggio automatico delle mail (anti-spam, quarantena di files riconosciuti come non sicuri ecc.) possono infatti subire elusioni. In questo caso il sistema genera automaticamente degli avvisi di anomalia ("alert" relativi a, in via esemplificativa, scarico di files pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) che vengono visualizzati dal Titolare del Trattamento. La finalità del controllo relativamente agli accessi a Internet è verificare se dai dati di connessione non risultino anomalie quali la violazione o l'elusione del sistema di blocco (Firewall) dei siti a contenuto illecito (es. siti a contenuto violento, discriminatorio, pornografico ecc.) o comunque non attinenti all'attività lavorativa.

La finalità del controllo relativo alla posta elettronica è verificare che l'e-mail aziendale venga utilizzata in conformità con le regole di condotta stabilite e quindi che non venga utilizzata per ricevere notifiche di messaggi da server esterni, non sicuri o comunque non attinenti all'attività lavorativa, per inviare a soggetti o indirizzi di posta elettronica non autorizzati informazioni e documenti riservati (es. invio di files a propri account di posta elettronica privati), per effettuare operazioni on-line non sicure e potenzialmente dannose non solo per la Società ma per lo stesso lavoratore (es. acquisti su siti Internet, download di files audio/video in violazione della legge sul copyright ecc.).

In caso di avviso di anomalia, la Società effettuerà un controllo anonimo sui dati aggregati riferito all'intera struttura aziendale oppure a sue aree, in modo da poter individuare l'area aziendale da richiamare al rispetto delle regole procedurali. Il controllo anonimo potrà

	Systems Projects Services srl	ITC-154596	
	Regolamento privacy e trattamento dati personali SPS	Sh. 22 of 22	Rev.0

concludersi con un avviso generalizzato relativo all'utilizzo anomalo di strumenti aziendali, con l'invito ad attenersi scrupolosamente alle istruzioni impartite a mezzo della presente procedura. Qualora il comportamento anomalo dovesse ripetersi o comunque nei casi di maggiore gravità (es. accesso a siti illegali o a contenuto discriminatorio o violento), la Società potrà effettuare controlli su base individuale ("Controllo Straordinario").

7.11.2. *Controllo straordinario*

Il secondo livello di controllo denominato "straordinario" viene attuato nei seguenti casi:

- a) nel caso in cui all'esito del controllo ordinario emergano comportamenti anomali ripetuti o comunque di particolare gravità (es. accesso a siti illegali o a contenuto discriminatorio o violento);
- b) nel caso vi sia l'esigenza di svolgere indagini di natura difensiva ovvero nel caso in cui sia necessario accertare, comportamenti che possano costituire reato o che siano comunque illeciti o non conformi alle disposizioni aziendali.

Il controllo straordinario potrà avvenire, laddove la natura dell'indagine lo richieda, anche mediante accesso diretto al PC del collaboratore che, su richiesta, dovrà consegnarlo al Titolare del Trattamento. Il controllo straordinario potrà altresì avvenire con la collaborazione di professionisti esterni (quali società di auditing, avvocati, consulenti informatici ecc.), mediante accesso al server e/o alla memoria di massa del computer dato in dotazione al collaboratore. Il controllo straordinario non potrà avere ad oggetto un arco temporale eccedente i dodici mesi precedenti la data in cui esso viene effettuato, salva la necessità di estendere l'indagine oltre tale periodo in ragione della natura del comportamento oggetto di indagine e/o in conseguenza di fatti emersi nel controllo relativo ai dodici mesi precedenti la data dell'indagine. In particolare, essendo i progetti e più in generale le attività di SPS complesse e articolate in più fasi che spesso ricoprono un lasso temporale anche di diversi anni, il tempo trascorso tra il primo verificarsi del problema e l'inizio dell'indagine potrebbe essere superiore rispetto a quello preventivato. Del suddetto controllo, verrà redatto processo verbale che dovrà riportare la data di inizio dell'indagine, il motivo dell'indagine, una descrizione sintetica delle attività di indagine svolta, il relativo arco temporale, la data della chiusura dell'indagine, se la conclusione dell'indagine richiede o meno l'instaurazione di un procedimento disciplinare. Il verbale di indagine dovrà essere sottoscritto dal responsabile del procedimento. Qualora non sia necessaria l'instaurazione di un procedimento disciplinare, sarà conservata copia del verbale di indagine mentre i relativi documenti cartacei (es. stampa delle e-mail, stampa dei siti internet visitati ecc.) dovranno essere distrutti, salvo che tali documenti siano necessari al fine di difendere un diritto della Società nei confronti di soggetti diversi dal collaboratore. Tale eventuale necessità di conservare i documenti cartacei di indagine anche in mancanza di procedimenti disciplinari dovrà essere indicata e motivata nel verbale di indagine. Qualora si ritenga di dover instaurare un procedimento disciplinare, i documenti raccolti nel corso dell'indagine potranno essere conservati sia su supporto informatico sia su supporto cartaceo, per il tempo necessario al fine di difendere i diritti della Società, connessi al procedimento disciplinare stesso e al suo esito. In caso di indagine da effettuarsi per ordine di una Pubblica Autorità, potranno essere effettuati controlli anche al di fuori della procedura di cui sopra secondo le modalità e con le procedure eventualmente prescritte dalla stessa Pubblica autorità. Resta inteso che entro 15 giorni dal completamento dell'indagine sarà data comunicazione alle RSA, se dovuta, e/o al lavoratore/collaboratore.