

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		SERVIZIO PREVENZIONE e PROTEZIONE	Numero revisione
		Numero pagina	1 di 47

Ai sensi del REGOLAMENTO (UE) 2016/679

MANUALE DI GESTIONE DELLA PRIVACY

DITTA	BURLANDI FRANCO S.R.L.
SEDE LEGALE	VIA di Passo Lombardo 257, 00133, Roma
PARTITA IVA	04571101007
SEDE LAVORATIVA	VIA DI PASSO LOMBARDO 257, 00133, Roma
DATORE DI LAVORO	Dr. Fabrizio Burlandi
ATTIVITÀ LAVORATIVE	Società di servizi e lavori

SOCIETÀ TITOLARE DEL TRATTAMENTO DATI	BURLANDI FRANCO S.R.L.
TITOLARE TRATTAMENTO DATI	Dr. Fabrizio Burlandi
D.P.O.	
RESPONSABILE AMMINISTRATIVO	Dr. Fabrizio Burlandi
Numero di Dipendenti	89

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	2 di 47

Sommario

Sommario.....	2
1 Inquadramento normativo, scopo e contenuti	3
2 Organigramma Aziendale	13
3 Descrizione attività – Registro del titolare e del responsabile del trattamento.....	14
4 Criteri di valutazione dei rischi e loro individuazione e mitigazione	22
4.1 Misure di sicurezza globali	22
Uso di internet da parte dei soggetti responsabili del trattamento	22
Uso di posta elettronica da parte dei soggetti responsabili del trattamento	22
Uso del FAX da parte dei soggetti responsabili del trattamento	22
Distruzione dei documenti da parte dei soggetti responsabili del trattamento	22
Gestione della posta cartacea ed elettronica da parte dei soggetti responsabili del trattamento.....	22
4.2 misure di sicurezza contro il rischio di distruzione o perdita dati	23
5 Procedura di formazione, scadenziario e notifica al garante	33
6 Responsabilità.....	34
7 Documentazione allegata.....	35
8 . Certificazione e sottoscrizione	36
ALLEGATO I.....	37
ALLEGATO II	38
ALLEGATO III.....	39
ALLEGATO IV:.....	40
ALLEGATO V:	41
ALLEGATO VI.....	42
ALLEGATO VII	43
ALLEGATO VIII.....	44
ALLEGATO IX:.....	45

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	3 di 47

1 Inquadramento normativo, scopo e contenuti

CODICE DI PROTEZIONE DELLA PRIVACY DAL 2004 FINO AL REGOLAMENTO (UE) 2016/679

Il codice per la protezione dei dati personali (comunemente noto anche come codice della privacy) è una norma della Repubblica Italiana, emanata con il Decreto legislativo 30 giugno 2003, n. 196, in vigore dal 1° gennaio 2004.

Il D.Lgs 196/2003 abroga la precedente legge 675/96, che era stata introdotta per rispettare gli Accordi di Schengen ed era entrata in vigore nel maggio 1997. Con il tempo, data la tipica stratificazione normativa che si produce nei sistemi giuridici a tradizione civilista (tra cui quello italiano), a tale norma si erano affiancate numerose altre disposizioni concernenti specifici aspetti del trattamento dei dati, che sono state conglobate nel Testo Unico vigente, entrato in vigore il 1° gennaio 2004.

Sull'applicazione della normativa vigila l'Autorità Garante per la protezione dei dati personali, istituita sin dalla L. 675/1996, poi confermata anche dal Testo Unico del 2003. Il decreto tutela il diritto del singolo sui propri dati personali e, conseguentemente, alla disciplina delle diverse operazioni di gestione (tecnicamente "trattamento") dei dati, riguardanti la raccolta, l'elaborazione, il raffronto, la cancellazione, la modificazione, la comunicazione o la diffusione degli stessi.

All'art.1 del testo unico viene riconosciuto il diritto assoluto di ciascuno sui propri dati, in cui si afferma testualmente: "Chiunque ha diritto alla protezione dei dati personali che lo riguardano". Tale diritto pertiene i diritti della personalità.

Il diritto alla riservatezza è diverso rispetto al diritto sui propri dati perché non riguarda solamente informazioni circa la propria vita privata, ma più in generale ingloba ogni informazione relativa ad una persona, pure se non coperta da riserbo (sono dati personali ad esempio il nome o l'indirizzo della propria abitazione).

Lo scopo della normativa è quello di evitare che il trattamento dei dati avvenga senza il consenso dell'avente diritto, ovvero in modo da recargli pregiudizio. Nel Testo Unico, Titolo II articoli da 8 a 10, sono a tal scopo definiti i diritti degli interessati, la modalità di raccolta e i requisiti dei dati, gli obblighi di chi raccoglie, detiene o tratta dati personali e le responsabilità e sanzioni in caso di danni.

Il 15 dicembre 2015, la Commissione Europea ha trovato l'accordo col Parlamento e col Consiglio UE per un testo unico sulla privacy che armonizza le normative degli Stati membri. L'accordo è composto da:

- una Direttiva sulla Protezione dei Dati (Data Protection Directive) per le forze di polizia e la magistratura;

- un Regolamento Generale sulla Protezione dei Dati (General Data Protection Regulation, GDPR), immediatamente esecutivo in tutta l'Unione Europea. È istituita un'unica autorità di vigilanza europea, si applica anche alle imprese con sede estera e operanti nell'Unione Europea, è previsto un tempo di adeguamento di due anni, e per le imprese non conformi sanzioni dal 2 al 4% del fatturato annuo.

Il Regolamento introduce il diritto all'oblio, il diritto alla portabilità dei dati fra diversi Service Provider, il diritto alla notifica dell'accesso abusivo di terzi a dati personali e sensibili particolarmente importanti.

Rev. 1 del 22/09/2020	Emesso da: Arnaldo Basilico	Approvato da: Fabrizio Burlandi
-----------------------	-----------------------------	---------------------------------

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	4 di 47

Le piccole e medie imprese (SME) non hanno più l'obbligo del responsabile della protezione dei dati (data protection officer), né l'obbligo di effettuare la valutazione dell'impatto (privacy impact assessment), a meno che non esista un rischio operativo non trascurabile.

Il 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il nuovo Regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation-Regolamento UE 2016/679), che è applicato definitivamente a decorrere dal 25 maggio 2018.

La definizione presente nell'articolo 4 stabilisce l'oggetto del regolamento: «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;

e la gestione stessa come: «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;

Cambia quindi la visione data oggi ai processi di marketing diretto, ma cambiano anche le modalità di registrazione e fruizione dei molti servizi internet; così varia anche la visione relativa alla profilazione dell'utente che non sarà più sufficiente, nel caso di questioni che hanno effetti giuridici, a deciderne una soluzione.

Riportiamo la definizione data dal Regolamento: «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;

Nel caso di marketing diretto l'interessato avrà sempre diritto di opporsi alle attività di profilazione. Inoltre è stato introdotto in modo chiaro il diritto all'oblio, cioè la cancellazione dei propri dati personali da parte di un titolare del trattamento qualora ad esempio cessino i motivi per cui si era dato il consenso.

Se ne pongono dei limiti di applicazione e si obbliga il titolare del trattamento ad agire tempestivamente perché l'informazione sia rimossa ovunque venga trattata.

La violazione dei dati personali (Data breach) non potrà essere una problematica solamente aziendale ma richiede maggiore informazione verso l'interessato e una comunicazione tempestiva ed obbligatoria verso l'autorità nazionale per la protezione dati.

Il modello che permette di trattare correttamente la gestione delle problematiche privacy nasce da modelli già esistenti e normati.

In particolare ci si rifà in primis alla normativa UNI EN ISO 9001 che definisce per un'organizzazione i requisiti di un sistema di gestione per la qualità ed in particolare la

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	5 di 47

creazione, all'interno dell'azienda, di un sistema organizzativo i cui requisiti rispettino tale norma.

Le metodologie e i requisiti previsti devono essere applicati a tutti i processi aziendali, dalla Produzione all'Area commerciale, dagli Acquisti alla Direzione Generale.

Il Sistema Qualità monitora tutto ciò che è previsto dalle procedure relative riportando le non conformità del processo dopo opportuna misurazione dei vari fenomeni.

Quindi viene prevista una metodologia che contempla la riduzione delle Non Conformità in un ciclo continuo di miglioramento.

L'azienda si è dotata di un Sistema Qualità in conformità alla normativa UNI EN ISO 9001 che si rivela utile nell'affrontare le metodologie per definire il proprio Sistema Privacy in quanto si parte da una medesima metodologia.

Il trattamento delle attività legate alla Privacy ricade fra gli eventi di Rischio e pertanto risulta compatibile con procedure, metodi, sistemi di controllo derivanti dall'applicazione di una qualsiasi valutazione del rischio.

Ogni elemento di Privacy viene quindi misurato dal punto di vista della probabilità di accadimento dei rischi connessi partendo comunque dal principio che, trattandosi di un rischio possibile, non si potranno mai realizzare processi atti ad eliminarlo completamente ma solamente a renderne minima la probabilità di accadimento.

Quindi si parlerà spesso di Non Conformità quando non vengono prese opportune decisioni in merito al trattamento del Rischio e tutto il sistema dovrà essere incentrato sulle politiche di mitigazione del Rischio.

Seguendo i dettami dei Sistemi Qualità si dovranno definire formalmente i responsabili Privacy (come da articolo 4 del GDPR):

il «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;

il «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;

l'azienda ha redatto un organigramma in modo da poter attribuire funzionalmente ogni risorsa ad una unità operativa, includendo non solo il personale dipendente ma tutti coloro che hanno una qualche attività con l'impresa stessa (ogni persona che può essere coinvolta in un processo di trattamento privacy).

Quindi, a partire dal censimento dei dati personali presenti e dei relativi trattamenti, è stato previsto per le singole risorse l'incarico di trattare quel particolare dato.

Per ogni risorsa è stata prevista una lettera di incarico che evidenzia compiti e responsabilità di trattamento e un piano formativo idoneo a preparare ad una corretta gestione.

La conservazione ed il trattamento del dato creano, come evidenziato in precedenza, eventi di rischio (accesso indesiderato, perdita, utilizzo non permesso, trattamento non conforme, ecc.).

viene quindi redatto nel presente manuale un PIA preventivo (Privacy Impact Assessment = censimento degli impatti privacy) in cui per ogni fenomeno si valuta rischiosità complessiva, azioni intraprese e rischiosità residua in modo da realizzare il primo documento che fotografa la situazione corrente.

Dalla valutazione del PIA nasce un piano interno in cui viene stabilito in quale modo verrà mitigato il singolo rischio, coloro che sono incaricati di operare in tal senso e il costo previsto per l'attività.

Rev. 1 del 22/09/2020	Emesso da: Arnaldo Basilico	Approvato da: Fabrizio Burlandi
-----------------------	-----------------------------	---------------------------------

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	6 di 47

Questo planning operativo viene costantemente monitorato e avrà impatto sul Privacy Impact Assessment successivo (una volta all'anno) in cui si andranno ad evidenziare i miglioramenti ottenuti e le eventuali ulteriori rischiosità subentrate.

Un PIA è disegnato per raggiungere normalmente tre obiettivi:

- Garantire la conformità con le normative, e requisiti di politica legali applicabili per la privacy;
- Determinare i rischi e gli effetti che ne conseguono;
- Valutare le protezioni e eventuali processi alternativi per mitigare i potenziali rischi per la privacy.

Non rappresenta quindi un mero strumento atto a censire, ma diventa l'elemento più importante per affermare di essere conformi alle prescrizioni del Regolamento.

Per la protezione informatica evidenziamo le funzioni che saranno generalmente implementate:

Individuazione: mappare le possibili situazioni di rischio dal punto di vista del tipo di violazione, delle risorse e delle unità organizzative coinvolte, della probabilità dell'evento e della gravità delle conseguenze;

Protezione: adottare in modo preventivo misure atte ad evitare trattamenti non necessari, ridurre la possibilità di accadimento, ridurre le eventuali conseguenze negative;

Rilevazione: istituire, secondo processi di qualità, un sistema di monitoraggio continuo in grado di segnalare tempestivamente eventi legati al rischio privacy;

Risposta: predisporre misure correttive adatte in caso di incidente informando gli interessati e l'autorità competente;

Ripristino: predisporre piani di ripristino della normale operatività

Il precedente Codice della Privacy permetteva, in taluni situazioni, formule per cui la mancanza di opposizione ad un trattamento diventa implicitamente un assenso. Ciò che definiamo silenzio assenso.

Il regolamento europeo, invece, si esprime definendo

«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.

Quindi, in ogni caso, l'interessato dovrà esprimersi in merito a trattamento fornendo un consenso effettivo ed inequivocabile, ad esempio, con dichiarazione scritta o attraverso mezzi elettronici o verbale (con registrazione).

Ogni operazione di comunicazione dovrà quindi far capo ad un preciso consenso formalizzato per ogni controparte presentabile nel caso l'interessato ne facesse richiesta.

L'interessato ha il diritto di revocare qualsiasi consenso abbia dato e deve essere informato di questo dal titolare del trattamento. Restano leciti tutti i trattamenti compiuti prima della revoca stessa.

In ottemperanza quindi al nuovo regolamento sopracitato vengono create:

1. Organigramma aziendale per le varie funzioni di tutela della privacy

Rev. 1 del 22/09/2020	Emesso da: Arnaldo Basilico	Approvato da: Fabrizio Burlandi
-----------------------	-----------------------------	---------------------------------

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	7 di 47

2. Censimento di tutte le operazioni di trattamento dati, loro valutazione del rischio e misure di mitigazione
3. Lettere di incarico del personale che maneggia dati soggetti a privacy
4. Formalizzazione della formazione del personale che maneggia dati soggetti a privacy
5. Formalizzazione ed archiviazione di tutte le comunicazioni dirette in materia di trattamento dati
6. Report periodici di verifica del corretto trattamento dati

A fronte dell'obiettivo di proteggere il dato personale e al cambiamento di scenario tecnologico che ha visto sempre più la distribuzione del dato mediante strumenti informatici privati e pubblici, si è dovuto provvedere a mettere in piedi sistemi atti a garantirne la protezione.

Fin dagli anni '90 sono stati prodotte le prime tecnologie in ambito ICT utili ad accrescere la protezione dei dati personali (PET = Privacy Enhancing Technologies).

L'attuale codice italiano sulla privacy (D.L 196/2003) nell'articolo 3 (Principio di necessità nel trattamento dei dati) fa riferimento a tali tecnologie:

I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Il nuovo regolamento compie un altro passo in avanti introducendo la Privacy by Design che con un innovativo approccio concettuale pone le basi della privacy del futuro.

L'articolo 25 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita) si esprime in tal senso:

1. 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.

Ovvero la nascita del sistema di protezione avviene contemporaneamente con l'evento di rischio di cui si deve fare trattamento e quindi non si fa trattamento fintantoché l'intero sistema non è stato definito.

È certamente una visione innovativa del problema che obbliga tutti coloro che introducono nuove rischiosità privacy sul mercato ad introdurre e certificare anche gli opportuni sistemi di sicurezza e di mitigazione del rischio.

Rev. 1 del 22/09/2020	Emesso da: Arnaldo Basilico	Approvato da: Fabrizio Burlandi
-----------------------	-----------------------------	---------------------------------

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	8 di 47

Nella progettazione delle basi dati si dovrà tener sempre conto di rendere minimo il dato personale utilizzato concentrandolo in chiaro in componenti limitate e protette applicando nel resto del progetto la pseudonimizzazione dell'informazione, definita come:

«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;

Attenzione quindi ai nuovi progetti software atti a realizzare strumenti per il trattamento del dato personale.

Il medesimo articolo 25 dice anche che:

2. 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.

Qui viene rappresentato il concetto di Privacy by Default dove si chiede di utilizzare il numero di informazioni necessario e sufficiente al trattamento in atto per limitare già in fase di progettazione il rischio privacy.

Fra gli altri compiti, il titolare e il responsabile del trattamento devono redigere i registri delle attività e dei trattamenti effettuati.

Formalmente la tenuta del registro rappresenta il sostituto della comunicazione diretta delle medesime informazioni al Garante della Privacy.

In realtà i registri da conservare e mantenere sono due:

- Il registro del titolare del trattamento, che contiene:
 - o Anagrafica del titolare stesso, di un contitolare se presente, del rappresentante e del titolare alla protezione dati;
 - o Le finalità del trattamento;
 - o Le categorie degli interessati a cui fa capo il dato;
 - o Eventuali termini per la cancellazione automatica del dato;
 - o Un'eventuale descrizione generale delle misure di sicurezza tecnico-organizzative.
- Il registro del responsabile del trattamento, in cui sono presenti:
 - o L'anagrafica dei responsabili del trattamento;
 - o La descrizione delle categorie di trattamento effettuati;
 - o Opzionalmente la descrizione delle misure di sicurezza intraprese.

La conservazione può avvenire in forma cartacea ma anche in forma elettronica rendendo sempre disponibile il dato ad eventuali ispezioni dell'autorità garante.

Rev. 1 del 22/09/2020	Emesso da: Arnaldo Basilico	Approvato da: Fabrizio Burlandi
-----------------------	-----------------------------	---------------------------------

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	9 di 47

Data Breach: che cosa fare in caso di violazione dei dati

«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;

Ai fini di evitare le violazioni dei dati personali vengono prese in considerazione le azioni da intraprendersi nel caso di perdita, distruzione, diffusione indebita di dati personali conservati, trasmessi o comunque trattati a causa di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi e altre calamità.

In particolare il testo del nuovo regolamento prevede l'obbligo di notifica all'autorità di controllo e la comunicazione della violazione al diretto interessato.

L'articolo 33 dice infatti:

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

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
 - a. descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
 - b. comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
 - c. descrivere le probabili conseguenze della violazione dei dati personali;
 - d. descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. 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. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

ed il 34:

Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

Rev. 1 del 22/09/2020	Emesso da: Arnaldo Basilico	Approvato da: Fabrizio Burlandi
-----------------------	-----------------------------	---------------------------------

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	10 di 47

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

Gli articoli 37, 38 e 39 (sezione 4) del GDPR trattano della figura del DPO (Data Protection Officer) in particolare della designazione, della posizione e dei compiti.

L'articolo 37 spiega che la figura del Data Protection Manager (DPO) non sempre è necessaria:

Designazione del responsabile della protezione dei dati

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

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	11 di 47

associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.

5. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.
6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.
7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Inoltre l'articolo seguente specifica che il DPO deve essere dotato di totale autonomia nella gestione delle problematiche affidate e devono essergli fornite risorse necessarie all'assolvimento dei compiti.

Viene peraltro visto come consulente interno per i temi privacy.

Posizione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.
4. Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.
6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

Si conclude con l'articolo che ne definisce l'attività:

Rev. 1 del 22/09/2020	Emesso da: Arnaldo Basilico	Approvato da: Fabrizio Burlandi
-----------------------	-----------------------------	---------------------------------

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	12 di 47

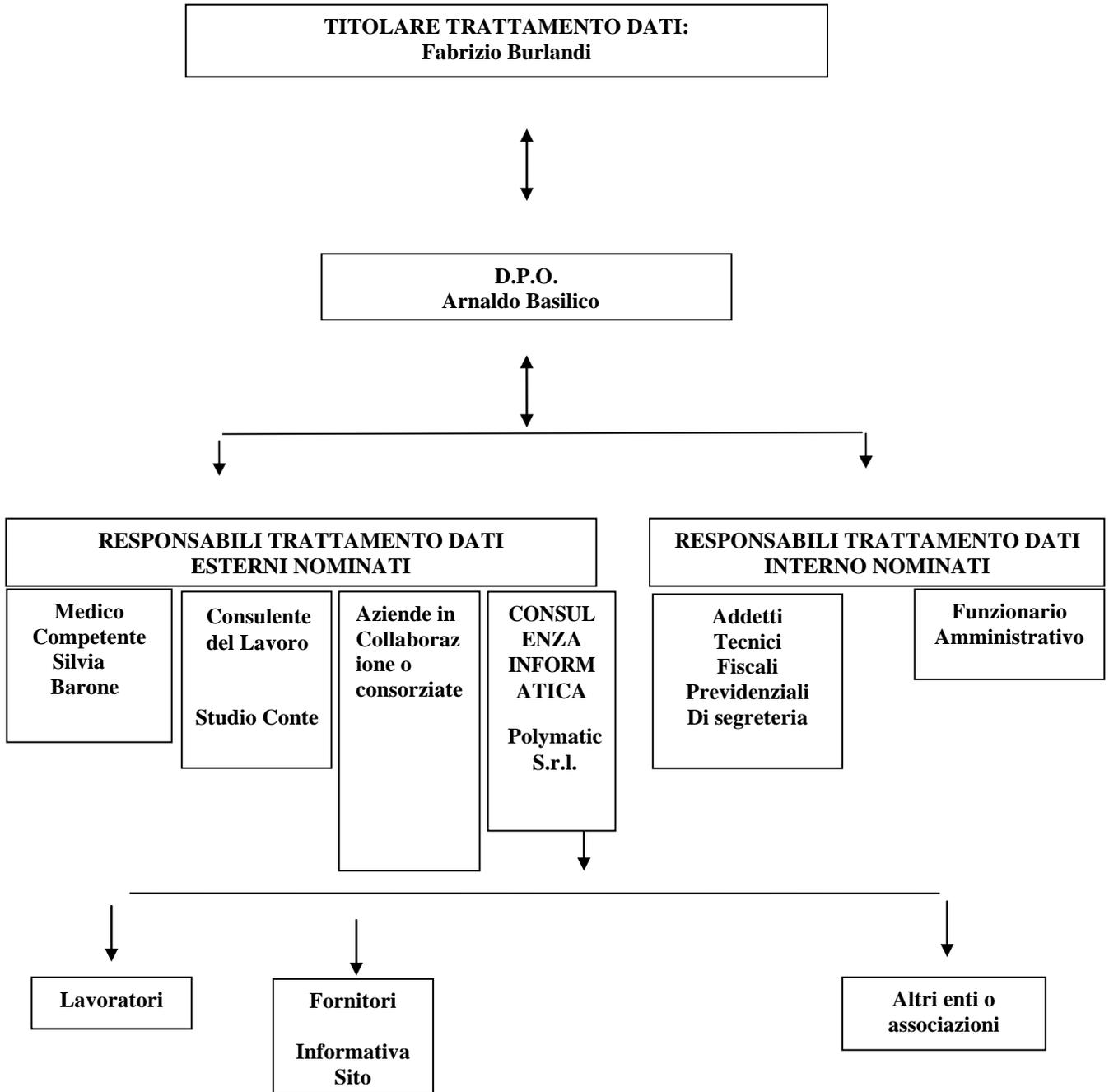
Compiti del responsabile della protezione dei dati

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

La figura del DPO è già presente sullo scenario internazionale da molti anni come un consulente interno o esterno esperto delle normative e delle problematiche privacy.

Per ovvie ragioni il DPO è una figura che non coinciderà con il CIO (responsabile informatico dell'azienda) in quanto si andrebbe normalmente in conflitto di interesse.

2 Organigramma Aziendale



Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	14 di 47

3 Descrizione attività – Registro del titolare e del responsabile del trattamento

TABELLA A SEDI IN CUI VENGONO TRATTATI I DATI		
Tipologia	Codice	Indirizzo
Sede legale	SL	VIA DI PASSO LOMBARDO n.259

TABELLA B CENSIMENTO DEI TRATTAMENTI E REPARTI IN CUI ESSO AVVIENE							
ID	Descrizione sintetica del trattamento	Categorie interessate Del trattamento	Natura dei dati	Strutture entro le quali avviene il trattamento	Luogo	Locale o reparto in cui avviene il trattamento	Formato dei dati trattati
T1	Assistenza lavorativa: <ul style="list-style-type: none"> • certificati handicap • denunce infortuni o malattie professionali • certificazioni e attestati 	Lavoratori E Clienti / Aziende associate	Sensibili Giudiziari	Uffici di segreteria	SL	Uffici di segreteria	Digitale Cartaceo
T2	Trattamento giuridico ed economico del personale dipendente: <ul style="list-style-type: none"> • raccolta iniziale dati dipendenti • stipula contratti di lavoro • rilevazione assenze personale • elaborazione buste paga • tenuta CV • istruzioni pratiche e domande di 	Lavoratori E Clienti / Aziende associate	Sensibili Giudiziari	Uffici di segreteria	SL	Uffici di segreteria	Digitale Cartaceo

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	15 di 47

	<ul style="list-style-type: none"> • pensione • denunce infortuni e • malattie professionali • gestione domande prestiti e anticipi TFR • pratiche procedimenti disciplinari • certificazioni personale • pratiche idoneità personale • pratiche Legge 104 • CU • Permessi sindacali • Gestione T.F.R. • Permessi congedi ferie • Rich / trasmissione documenti personali • Riscatto pensione o liquidazione • Sciopero 						
T3	Gestione fornitori di beni e servizi	Fornitori	Personali	Uffici di segreteria	SL	Uffici di segreteria	Digitale Cartaceo
T4	Gestione posta elettronica o cartacea	Tutti	Personali	Uffici di segreteria	SL	Uffici di segreteria	Digitale Cartaceo

Alcuni trattamenti dei dati personali possono essere affidati all'esterno della struttura del titolare:

TABELLA C				
CENSIMENTO DEI TRATTAMENTI AFFIDATI ALL'ESTERNO				
ID	Descrizione sintetica del trattamento	Trattamenti interessati	Soggetto esterno	Descrizione criteri ed impegni assunti dal soggetto esterno per l'adozione delle misure minime
E1	Adempimenti in materia di diritto del lavoro E di tipo legale	T1 e T2	Studio consulenza STUDIO CONTE	Il soggetto assume l'incarico ai sensi del REGOLAMENTO (UE) 2016/679 di responsabile "esterno" del trattamento dei dati personali e si obbliga ai doveri di riservatezza e di organizzazione previsti dalle normative in vigore per chi esercita il trattamento dati personali in proprio o per conto terzi.

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	16 di 47

E2	Attività di sorveglianza sanitaria MEDICO COMPETENTE (D.Lgs 81/2008)	T1 e T2	Studio medico DOTT. SILVIA BARONE	Il soggetto assume l'incarico ai sensi del REGOLAMENTO (UE) 2016/679 di responsabile "esterno" del trattamento dei dati personali e si obbliga ai doveri di riservatezza e di organizzazione previsti dalle normative in vigore per chi esercita il trattamento dati personali in proprio o per conto terzi.
E3	Attività di gestione informatica	T4	Altre aziende di consulenza software POLYMATIC S.R.L.	Il soggetto assume l'incarico ai sensi del REGOLAMENTO (UE) 2016/679 di responsabile "esterno" del trattamento dei dati personali e si obbliga ai doveri di riservatezza e di organizzazione previsti dalle normative in vigore per chi esercita il trattamento dati personali in proprio o per conto terzi.
E4	Adempimenti e formazione in tema di sicurezza sul lavoro (D.Lgs 81/2008)	T3	HIDEA!	Il soggetto assume l'incarico ai sensi del REGOLAMENTO (UE) 2016/679 di responsabile "esterno" del trattamento dei dati personali e si obbliga ai doveri di riservatezza e di organizzazione previsti dalle normative in vigore per chi esercita il trattamento dati personali in proprio o per conto terzi.
E5	Adempimenti e formazione in tema di trattamento delle acque	T3	\	Il soggetto assume l'incarico ai sensi del REGOLAMENTO (UE) 2016/679 di responsabile "esterno" del trattamento dei dati personali e si obbliga ai doveri di riservatezza e di organizzazione previsti dalle normative in vigore per chi esercita il trattamento dati personali in proprio o per conto terzi.
E6	Newsletter, ufficio stampa	T3	\	Il soggetto assume l'incarico ai sensi del REGOLAMENTO (UE) 2016/679 di responsabile "esterno" del trattamento dei dati personali e si obbliga ai doveri di riservatezza e di organizzazione previsti dalle normative in vigore per chi esercita il trattamento dati personali in proprio o per conto terzi.
E7	Analisi dei terreni dei clienti	T3	\	Il soggetto assume l'incarico ai sensi del REGOLAMENTO (UE) 2016/679 di responsabile "esterno" del trattamento dei dati personali e si obbliga ai doveri di riservatezza e di organizzazione previsti dalle normative in vigore per chi esercita il trattamento dati personali in proprio o per conto terzi.
E8	Normativa sulla privacy	T3	\	Il soggetto assume l'incarico ai sensi del REGOLAMENTO (UE) 2016/679 di responsabile "esterno" del trattamento dei dati personali e si

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	17 di 47

				obbliga ai doveri di riservatezza e di organizzazione previsti dalle normative in vigore per chi esercita il trattamento dati personali in proprio o per conto terzi.
--	--	--	--	---

In considerazione dell'impossibilità di eseguire controlli e verifiche presso strutture esterne alla propria, il titolare del trattamento dati ritiene adeguato richiedere al soggetto esterno, a garanzia della corretta esecuzione del trattamento, un'autocertificazione dell'osservanza dei criteri dettati dal REGOLAMENTO (UE) 2016/679 quali "minimi" per eseguire un trattamento dati.

Resta comunque salvo l'obbligo per tutti gli incaricati del trattamento dati che intrattengono rapporti con soggetti esterni, di richiamare all'osservanza delle misure minime nonché di segnalare, senza ritardo alcuno, al responsabile del trattamento, eventuali difformità rispetto a quanto autocertificato.

TABELLA B 2					
DESCRIZIONE ULTERIORE DEI TRATTAMENTI DEI DATI PERSONALI INTERNI ALLA STRUTTURA DEL TITOLARE, CHE AVVENGONO MEDIANTE L'USO DI STRUMENTI INFORMATICI					
ID	Denominazione banca dati	Luogo di custodia	Tipo e luogo di custodia dei supporti back-up	Tipologia dispositivi di accesso	Tipologia di interconnessione
T1	Assistenza lavorativa: <ul style="list-style-type: none"> • certificati handicap • denunce infortuni o malattie professionali • certificazioni e attestati 	SERVER	I supporti di back up vengono custoditi dall'incaricato in maniera sicura dai rischi connessi alla diffusione ed alla distribuzione degli stessi	PC equipaggiati con sistemi operativi e programmi adeguati	LAN
T2	Trattamento giuridico ed economico del personale dipendente: <ul style="list-style-type: none"> • raccolta iniziale dati dipendenti • stipula contratti di lavoro • rilevazione assenze personale • elaborazione buste paga • tenuta CV • istruzioni pratiche e di domande pensione • denunce infortuni e malattie 	SERVER	I supporti di back up vengono custoditi dall'incaricato in maniera sicura dai rischi connessi alla diffusione ed alla distribuzione degli stessi	PC equipaggiati con sistemi operativi e programmi adeguati	LAN

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	18 di 47

	<ul style="list-style-type: none"> professionali • gestione domande prestiti e anticipi TFR • pratiche procedimenti disciplinari • certificazioni personale • pratiche idoneità personale • pratiche Legge 104 • CUD • Permessi sindacali • Gestione T.F.R. • Permessi congedi ferie • Rich / trasmissione documenti personali • Riscatto pensione liquidazione o • Sciopero 				
T3	Gestione fornitori di beni e servizi	SERVER	I supporti di back up vengono custoditi dall'incaricato in maniera sicura dai rischi connessi alla diffusione ed alla distribuzione degli stessi	PC equipaggiati con sistemi operativi e programmi adeguati	LAN
T4	Gestione posta elettronica o cartacea	SERVER	I supporti di back up vengono custoditi dall'incaricato in maniera sicura dai rischi connessi alla diffusione ed alla distribuzione degli stessi	PC equipaggiati con sistemi operativi e programmi adeguati	LAN

TABELLA B3							
DESCRIZIONE ULTERIORE DEI TRATTAMENTI DEI DATI PERSONALI INTERNI ALLA STRUTTURA DEL TITOLARE, CHE <u>NON</u> AVVENGONO MEDIANTE L'USO DI STRUMENTI INFORMATICI							
ID	Denominazione banca dati	Luogo di custodia dei	Sistema di protezione	Sistema di sicurezza	Luogo di	Sistema di protezione	Sistema di sicurezza

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A.	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE	REGOLAMENTO (UE) 2016/679	Numero pagina	19 di 47

		dati cartacei	accesso	anti- distruzione previsto	archiviazione storica	accesso	anti- distruzione previsto
T1	Assistenza lavorativa: <ul style="list-style-type: none"> • certificati handicap • denunce infortuni o malattie professionali • certificazioni e attestati 	ARMADI CHIUSI DI SEGRETERIA	Chiave / serratura / allarme principale uffici	Estintore	ARCHIVIO CHIUSO A CHIAVE	Chiave / serratura	Estintore
T2	Trattamento giuridico ed economico del personale dipendente: <ul style="list-style-type: none"> • raccolta iniziale dati dipendenti • stipula contratti di lavoro • rilevazione assenze personale • elaborazione buste paga • tenuta CV • istruzioni pratiche e di domande di pensione • denunce infortuni e malattie professionali • gestione domande prestiti e anticipi TFR • pratiche procedimenti disciplinari • certificazioni personale • pratiche idoneità personale • pratiche Legge 104 • CUD • Permessi sindacali • Gestione T.F.R. • Permessi congedi ferie • Rich / trasmissione documenti personali • Riscatto pensione o 	ARMADI CHIUSI DI SEGRETERIA	Chiave / serratura / allarme principale uffici	Estintore	ARCHIVIO CHIUSO A CHIAVE	Chiave / serratura	Estintore

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	20 di 47

	liquidazione • Sciopero						
T3	Gestione fornitori di beni e servizi	ARMADI CHIUSI DI SEGRETERIA	Chiave / serratura / allarme principale uffici	Estintore	ARCHIVIO CHIUSO A CHIAVE	Chiave / serratura	Estintore
T4	Gestione posta elettronica o cartacea	ARMADI CHIUSI DI SEGRETERIA	Chiave / serratura / allarme principale uffici	Estintore	ARCHIVIO CHIUSO A CHIAVE	Chiave / serratura	Estintore

INDIVIDUAZIONE DEI SOGGETTI DEL TRATTAMENTO

Il trattamento dei dati personali deve avvenire esclusivamente a cura di taluni soggetti ben identificati dalla legge, nessuno al di fuori di questa sfera di soggetti è autorizzato a venire a contatto con dei dati personali.

ORGANIGRAMMA SOGGETTI INTRESSATI AL TRATTAMENTO DATI				
Titolare del trattamento	Persona giuridica nella persona del suo legale rappresentante	Nome e cognome	Attilio Tocchi	Individuato “OPE LEGIS”
		Ruolo	Amministratore	
		Luogo di riferimento	Tutte le sedi	
D.P.O. Data Protection Officer	Responsabile protezione dati, Individuato personalmente dal titolare del trattamento dati anche sulla base delle conoscenze acquisite	Nome e cognome	Maestrini Stefano	Nominato con lettera di incarico
		Ruolo	Consulente in tema di Privacy	
		Luogo di riferimento	Tutte le sedi	
Responsabile del trattamento per la segreteria	Individuato personalmente dal titolare del trattamento dati	Nome e cognome	Paolo Rossi	Nominato con lettera di incarico
		Ruolo	Direttore	
		Luogo di riferimento	Tutte le sedi	
Custode delle parole chiave e delle chiavi degli armadi	Individuato personalmente dal titolare del trattamento dati	Nome e cognome	Paolo Rossi	Nominato con lettera di incarico
		Ruolo	Direttore	
		Luogo di	Tutte le sedi	

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	21 di 47

		riferimento		
Custode delle parole chiave e delle chiavi degli armadi	Individuato personalmente dal titolare del trattamento dati	Nome e cognome	Paolo Rossi	Nominato con lettera di incarico
		Ruolo	Direttore	
		Luogo di riferimento	Tutte le sedi	
Incaricato del back-up	Individuato personalmente dal titolare del trattamento dati	Nome e cognome	Paolo Rossi e Ditta SIGES Ditta ERREPI ELABORAZIONE DATI SRL	Personale Nominato con lettera di incarico
		Ruolo	Direttore	
		Luogo di riferimento	Tutte le sedi	
Amministratore di sistema	Individuato personalmente dal titolare del trattamento dati	Nome e cognome	Paolo Rossi e Ditta SIGES Ditta ERREPI ELABORAZIONE DATI SRL	Personale Nominato con lettera di incarico
		Ruolo	Direttore	
		Luogo di riferimento	Tutte le sedi	
Addetti protezione dati	Individuato personalmente dal titolare del trattamento dati	Nome e cognome	Tutti i dipendenti	Nominato con lettera di incarico
		Ruolo	-	
		Luogo di riferimento	Tutte le sedi	

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	22 di 47

4 Criteri di valutazione dei rischi e loro individuazione e mitigazione

4.1 Misure di sicurezza globali

Uso di internet da parte dei soggetti responsabili del trattamento:

il corretto uso di internet rappresenta uno dei punti cardine per la sicurezza della infrastruttura informatica entro la quale si effettua il trattamento dati.

Il momento critico è sempre quello del “download” di software o dati al di fuori dei casi espressamente consentiti dal Titolare del trattamento.

L’incaricato al trattamento dati deve astenersi dal compiere “download” non autorizzati, oppure aprire link di siti internet non sicure onde prevenire situazioni critiche come la presenza di Virus, Spam, malware, etc. nel PC che possono esporre a rischio i dati personali presenti.

Uso di posta elettronica da parte dei soggetti responsabili del trattamento:

il corretto uso della posta elettronica può essere assimilato a quanto già espresso per l’uso di internet, in quanto il momento critico è sempre quello del “download” di software o dati al di fuori dei casi espressamente consentiti dal Titolare del trattamento.

Uso del FAX da parte dei soggetti responsabili del trattamento:

I documenti in ingresso via FAX, che contengano dati personali, devono essere trattati con particolare cura, affinché non restino a disposizione dei soggetti non autorizzati. L’incaricato della gestione di tali documenti deve vigilare sulla corretta esecuzione della procedura di smistamento.

Distruzione dei documenti da parte dei soggetti responsabili del trattamento:

I documenti cartacei contenenti dati personali saranno distrutti o resi illeggibili una volta arrivati a scadenza, da apposito distruggi documenti o mezzo idoneo.

Gestione della posta cartacea ed elettronica da parte dei soggetti responsabili del trattamento:

La posta cartacea ricevuta viene ritirata dall’addetto (Responsabile trattamento amministrativo) e smistata a chi di competenza, la consegna deve avvenire con la busta ancora sigillata.

Se è necessaria la sua apertura, essa viene protocollata, e immediatamente consegnata al diretto interessato.

La posta elettronica o via PEC ricevuta viene aperta dall’addetto (Responsabile trattamento amministrativo) e smistata a chi di competenza, nel modo e maniera indicato dal diretto interessato (forma cartacea o inoltrata ad altro indirizzo email).

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	23 di 47

4.2 misure di sicurezza contro il rischio di distruzione o perdita dati

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il DPO può stabilire la periodicità con cui devono essere effettuate le copie di sicurezza delle banche dati trattati. I criteri devono essere stabiliti dal DPO in relazione al tipo di rischio potenziale e in base al livello di tecnologia.

Procedura di esecuzione del back-up:

Il DPO nomina con lettera di incarico il responsabile della procedura di backup, il quale deve essere in grado di poter lavorare ed effettuare i dovuti passaggi in completa autonomia per l'attuazione del salvataggio delle copie negli archivi informatici.

La procedura deve essere programmata e completamente automatica al fine di evitare imperizie o dimenticanze dell'operatore.

I backup contenenti i dati devono essere protetti da:

- Agenti chimici
- Fonti di calore
- Campi magnetici
- Intrusione ed atti vandalici
- Incendio
- Allagamento
- Furto

Nel caso in cui i supporti del backup siano dismessi essi devono essere formattati in modo che i dati in essi contenuti siano resi illeggibili e cancellati.

I dati informatici sono comunque ospitati nei PC e Server della sede amministrativa, protetto da sistemi antivirus, antispam, sono custoditi all'interno di un luogo allarmato contro le effrazioni. .

La ditta Polymatic S.r.l., invece, offre assistenza software specializzata per alcuni programmi installati

I programmi e sistemi operativi vengono aggiornati con regolarità.

Virus Informatici:

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o di perdita a causa di virus informatici, il DPO stabilisce quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.

Il DPO stabilisce inoltre la periodicità, non superiore a sei mesi, con cui debbono essere effettuati gli aggiornamenti dei sistemi antivirus utilizzati per ottenere un accettabile standard di sicurezza delle banche dati trattate.

I criteri debbono essere definiti dal DPO in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata. In particolare per ogni sistema debbono essere definite le seguenti specifiche:

- Il tipo di programma utilizzato;
- La periodicità degli aggiornamenti.

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	24 di 47

Nel caso in cui su uno o più sistemi si dovesse verificare la perdita di informazioni o danni a causa di infezione o contagio da virus informatici il DPO deve provvedere ad attivare tutti i sistemi di risanamento idonei al recupero dell'elaboratore infetto, all'impedimento della propagazione del virus ed alla protezione della rete da attacchi futuri analoghi.

ASSEGNAZIONE NOMI UTENTE

Il DPO deve definire le modalità di assegnazione dei nomi identificativi per consentire a ciascun Incaricato del trattamento di accedere ai sistemi di trattamento delle banche di dati.

Non sono ammessi nomi identificativi di gruppo, con la sola eccezione dei pochi identificativi assegnati per l'amministrazione di sistema, relativamente ai sistemi operativi che prevedono un unico livello di accesso.

In ogni caso, un codice identificativo assegnato ad un Incaricato del trattamento deve essere annullato se l'Incaricato del trattamento ha dato le dimissioni.

ASSEGNAZIONE DELLE PASSWORD

Il DPO deve definire le modalità di assegnazione delle password e decidere che ogni utente Incaricato del trattamento possa modificare autonomamente la propria password di accesso.

In questo caso la modifica richiede che venga data comunicazione al Custode della password e al DPO (se diverso dal Custode delle password).

SICUREZZA DELLE TRASMISSIONI DATI

Al fine di garantire la sicurezza delle trasmissioni dei dati su rete pubblica, il DPO stabilisce le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione su ogni sistema collegato in rete pubblica.

I criteri debbono essere definiti dal DPO in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Il presente documento è costantemente aggiornato ad opera del DPO circa ogni variazione dell'elenco degli Incaricati del trattamento autorizzati al trattamento dei dati personali.

In particolare, in caso di trattamento automatizzato di dati, per ogni Incaricato del trattamento deve essere indicato lo USER ID assegnato.

In caso di dimissioni di un Incaricato del trattamento o di revoca delle autorizzazioni al trattamento dei dati, il DPO deve darne immediata comunicazione al Custode delle password (se diverso dal DPO) che provvederà a disattivare la possibilità di accesso al sistema per il soggetto in questione.

Al DPO è affidato il compito di verificare ogni anno, entro il 31 Dicembre, le autorizzazioni di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati.

Al DPO è affidato il compito di redigere e di aggiornare ad ogni variazione la Tabella dei permessi di accesso che indica per ogni banca di dati i tipi di permesso di accesso per ogni Incaricato del trattamento autorizzato.

In particolare, per ogni Incaricato del trattamento e per ogni banca dati debbono essere indicati i privilegi assegnati tra seguenti:

- I. Inserimento dei dati;
- II. Lettura e stampa dei dati;
- III. Modifica di dati;

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	25 di 47

IV. Cancellazione di dati.

MANUTENZIONE DELLE APPARECCHIATURE

Al DPO è affidato il compito di verificare ogni anno la situazione delle apparecchiature installate con cui vengono trattati i dati, delle apparecchiature periferiche e, in particolare, dei dispositivi di collegamento con le reti pubbliche.

La verifica ha lo scopo di controllare l'affidabilità del sistema per quanto riguarda:

- La sicurezza dei dati trattati;
- Il rischio di distruzione o di perdita;
- Il rischio di accesso non autorizzato o non consentito, tenendo conto anche dell'evoluzione tecnologica.

Al DPO è affidato il compito di verificare ogni anno la situazione dei Sistemi Operativi installati sulle apparecchiature con le quali vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi per quanto riguarda:

- La sicurezza dei dati trattati;
- Il rischio di distruzione o di perdita;
- Il rischio di accesso non autorizzato o non consentito, tenendo conto in particolare di:
- Disponibilità di nuove versioni migliorative dei Sistemi operativi utilizzati;
- Segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

Nel caso in cui esistano rischi evidenti il DPO deve informare il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurarne il corretto trattamento dei dati in conformità alle norme in vigore.

Al DPO è affidato il compito di verificare ogni anno la situazione delle applicazioni installate sulle apparecchiature con le quali vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità del software applicativo, per quanto riguarda:

- La sicurezza dei dati trattati;
- Il rischio di distruzione o di perdita;
- Il rischio di accesso non autorizzato o non consentito, tenendo conto in particolare della disponibilità di nuove versioni migliorative delle applicazioni installate che consentano maggiore sicurezza contro i rischi di intrusione o di danneggiamento dei dati.

Nel caso in cui esistano rischi evidenti il DPO deve informarne il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

IL PIANO DEI RISCHI

Momento fondamentale e qualificante del presente documento è quello della valutazione specifica dei rischi, tipici dell'infrastruttura oggetto di analisi, incombenti sui dati.

Per una trattazione più analitica della materia, suddividiamo l'analisi dei rischi in funzione delle 4 tipologie classiche di rischiosità incombente sui dati :

- Rischi riconducibili al cattivo comportamento degli operatori
- Rischi riconducibili al malfunzionamento delle apparecchiature
- Rischi riconducibili ad eventi fisici ed atmosferici
- Rischi specifici cui sono sottoposte le risorse connesse in rete internet

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	26 di 47

EVENTI DANNOSI IN SEGUITO A CATTIVO COMPORTAMENTO DEGLI OPERATORI O DI SOGGETTI TERZI

ANALISI DEI RISCHI					
Descrizione del rischio	Probabilit dell'event	Trattament interessato (6)	Misura di sicurezza adottata	Tipologia Della misura	Responsabile dell'attuazione della misura
Danneggiamento volontario	BASSA	TUTTI	Vigilanza sugli operatori	PREVENTIVA / DI CONTENIMENTO DEGLI EFFETTI DANNOSI	TITOLARE / D.P.O.
Furto	BASSA	TUTTI	Vigilanza sugli operatori Installazione di un sistema antifurto o di sistemi anti intrusione nei locali ove sono tenuti i dati. Adozione di tecniche di cifratura dei dati	PREVENTIVA / DI CONTRASTO	TITOLARE / D.P.O.
Uso non autorizzato di supporti di memorie	MEDIA	TRATTAM. INFORM.	Vigilanza sugli operatori e configurazione di utenze non amministrative. Adozione di tecniche di cifratura dei dati	PREVENTIVA	TITOLARE / D.P.O. / INCARICATO MANUTENZ.
Errore del personale operativo	MEDIA	TUTTI	Vigilanza sugli operatori ed organizzazione corsi di formazione	PREVENTIVA	TITOLARE / D.P.O.
Errore di manutenzione	MEDIA	TRATTAM. INFORM.	Impiego di personale specializzato	PREVENTIVA	TITOLARE / D.P.O. / INCARICATO MANUTENZ.
Uso illegale di software	MEDIA	TRATTAM. INFORM.	Vigilanza sugli operatori e configurazione di utenze non amministrative	PREVENTIVA	TITOLARE / D.P.O. / INCARICATO MANUTENZ.
Accesso non autorizzato alla rete	BASSA	TRATTAM. INFORM.	Configurazione di utenze protette da password	PREVENTIVA	TITOLARE / D.P.O. / INCARICATO MANUTENZ.
Indirizzamento non corretto della posta elettronica	MEDIA	TRATTAM. INFORM.	Vigilanza sul personale e formazione dello stesso	PREVENTIVA	D.P.O.
Sottrazione di credenziali di autenticazione	MEDIA	TRATTAM. INFORM.	Configurazione di un sistema di cambio periodico della password e di disattivazione in caso di prolungato non impiego dell'utenza	PREVENTIVA	TITOLARE / D.P.O. / INCARICATO MANUTENZ.
Visione da parte di soggetti non autorizzati di dati cartacei dopo la loro eliminazione	MEDIA	TRATTAM. CARTACEI	Impiego di un distruggidocumenti o di altro metodo per rendere illeggibili tutti i fogli contenenti dati personali	DI CONTRASTO	TITOLARE / D.P.O. /
Lettura da parte di soggetti non	MEDIA	TRATTAM. INFORM.	Impiego di un distruggi-CD o di altro metodo di	DI CONTRASTO	TITOLARE / D.P.O. /

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	27 di 47

autorizzati di dati digitali su supporti magnetici dopo la loro dismissione			annullamento dei supporti ditta di manutenzione attrezzata con smagnetizzatore HD		
---	--	--	---	--	--

EVENTI DANNOSI IN SEGUITO A MALFUNZIONAMENTO DELLE APPARECCHIATURE

ANALISI DEI RISCHI					
Descrizione del rischio	Probabilità dell'evento	Trattament interessato (6)	Misura di sicurezza adottata	Tipologia Della misura	Responsabile dell'attuazione della misura
Guasto hardware	MEDIA	TRATTAM. INFORM.	Continua manutenzione delle apparecchiature	PREVENTIVA / DI CONTENIMENTO DELL'EVENTO DANNOSO	TITOLARE / D.P.O./ INCARICATO MANUTENZ
Linea elettrica instabile	BASSA	TRATTAM. INFORM.	Installazione di unità di continuità elettrica stabilizzate	PREVENTIVA / DI CONTENIMENTO DELL'EVENTO DANNOSO	TITOLARE / D.P.O./ INCARICATO MANUTENZ
Guasto tecnico al provider di rete	MEDIA	TRATTAM. INFORM.	Conclusione di contratti di somministrazione del servizio con provider certificati	PREVENTIVA	TITOLARE / D.P.O./
Danni sulle linee Di rete	BASSA	TRATTAM. INFORM.	Certificazione realizzazione impianto secondo le regole dell'arte	PREVENTIVA	TITOLARE / D.P.O./ INCARICATO MANUTENZ
Guasto software	MEDIA	TRATTAM. INFORM.	Continua manutenzione delle apparecchiature	PREVENTIVA / DI CONTENIMENTO DELL'EVENTO DANNOSO	TITOLARE / D.P.O./ INCARICATO MANUTENZ
Azione di virus informatici o di altri malware	MEDIA	TRATTAM. INFORM	Installazione di un software antivirus di rete adeguato Contratto con ditta di manutenzione	PREVENTIVA / DI CONTENIMENTO DELL'EVENTO DANNOSO	TITOLARE / D.P.O./ INCARICATO MANUTENZ
Spamming e tecniche di sabotaggio informatico	MEDIA	TRATTAM. INFORM	Installazione di un sistema di firewalling dimensionato sulla struttura Contratto con ditta di manutenzione	PREVENTIVA / DI CONTENIMENTO DELL'EVENTO DANNOSO	TITOLARE / D.P.O./ INCARICATO MANUTENZ
Degrado delle apparecchiature	MEDIA	TRATTAM. INFORM.	Continua manutenzione e redazione di un piano di sostituzioni Contratto con ditta di manutenzione	PREVENTIVA	TITOLARE / D.P.O./ INCARICATO MANUTENZ
Intercettazioni di informazioni di rete	MEDIA	TRATTAM. INFORM.	Installazione di un sistema di firewalling dimensionato sulla struttura e adozione di policy di rete corrette	PREVENTIVA	TITOLARE / D.P.O./ INCARICATO MANUTENZ

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	28 di 47

EVENTI DANNOSI IN SEGUITO A MALFUNZIONAMENTO DELLE APPARECCHIATURE

ANALISI DEI RISCHI					
Descrizione del rischio	Probabilità dell'evento	Trattament interessato (6)	Misura di sicurezza adottata	Tipologia Della misura	Responsabile dell'attuazione della misura
Guasto hardware	MEDIA	TRATTAM. INFORM.	Continua manutenzione delle apparecchiature Contratto con ditta di manutenzione	PREVENTIVA / DI CONTENIMENTO DELL'EVENTO DANNOSO	TITOLARE / D.P.O./ INCARICATO MANUTENZ
Linea elettrica instabile	MEDIA	TRATTAM. INFORM.	Installazione di unità di continuità elettrica stabilizzate	PREVENTIVA / DI CONTENIMENTO DELL'EVENTO DANNOSO	TITOLARE / D.P.O./ INCARICATO MANUTENZ
Guasto tecnico al provider di rete	MEDIA	TRATTAM. INFORM.	Conclusione di contratti di somministrazione del servizio con provider certificati	PREVENTIVA	TITOLARE / D.P.O./
Danni sulle linee Di rete	BASSA	TRATTAM. INFORM.	Certificazione realizzazione impianto secondo le regole dell'arte	PREVENTIVA	TITOLARE / D.P.O./ INCARICATO MANUTENZ
Guasto software	MEDIA	TRATTAM. INFORM.	Continua manutenzione delle apparecchiature Contratto con ditta di manutenzione	PREVENTIVA / DI CONTENIMENTO DELL'EVENTO DANNOSO	TITOLARE / D.P.O./ INCARICATO MANUTENZ
Azione di virus informatici o di altri malware	MEDIA	TRATTAM. INFORM.	Installazione di un software antivirus di rete adeguato Contratto con ditta di manutenzione	PREVENTIVA / DI CONTRASTO /DI CONTENIMENTO DELL'EVENTO DANNOSO	TITOLARE / D.P.O./ INCARICATO MANUTENZ
Spamming e tecniche di sabotaggio informatico	MEDIA	TRATTAM. INFORM.	Installazione di un sistema di firewalling dimensionato sulla struttura Contratto con ditta di manutenzione	PREVENTIVA / DI CONTRASTO /DI CONTENIMENTO DELL'EVENTO DANNOSO	TITOLARE / D.P.O./ INCARICATO MANUTENZ
Degrado delle apparecchiature	MEDIA	TRATTAM. INFORM.	Continua manutenzione e redazione di un piano di sostituzioni Contratto con ditta di manutenzione	PREVENTIVA	TITOLARE / D.P.O./ INCARICATO MANUTENZ
Intercettazioni di informazioni di rete	MEDIA	TRATTAM. INFORM.	Installazione di un sistema di firewalling dimensionato sulla struttura e adozione di policy di rete	PREVENTIVA	TITOLARE / D.P.O./ INCARICATO MANUTENZ

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	29 di 47

		corrette	
--	--	----------	--

EVENTI DANNOSI IN SEGUITO AD EVENTI FISICI ED ATMOSFERICI

ANALISI DEI RISCHI					
Descrizione del rischio	Probabilità dell'evento	Trattament interessato (6)	Misura di sicurezza adottata	Tipologia Della misura	Responsabile dell'attuazione della misura
Inondazione	BASSA	TUTTI	I SERVER ed in generale i dispositivi contenenti dati sono posti su supporti rialzati	DI CONTRASTO / DI CONTENIMENTO DELL'EVENTO DANNOSO	TITOLARE / D.P.O./
Fulmine	BASSA	TRATTAM. INFORM.	Installazione di unità di continuità elettrica stabilizzate	DI CONTENIMENTO DELL'EVENTO DANNOSO	TITOLARE / D.P.O./
Fuoco	BASSA	TRATTAM. INFORM.	I SERVER ed in generale i dispositivi contenenti dati sono installati in locali dotati di estintore o di sistema anti-incendio	DI CONTRASTO DELL'EVENTO DANNOSO	TITOLARE / D.P.O./
Temperatura ed umidità eccessive	MEDIA	TRATTAM. INFORM.	I SERVER ed in generale i dispositivi contenenti dati sono posti all'interno di locali chiusi	DI CONTRASTO / DI CONTENIMENTO DELL'EVENTO DANNOSO	TITOLARE / D.P.O./ INCARICATO MANUTENZ
Polvere	MEDIA	TRATTAM. INFORM.	I SERVER ed in generale i dispositivi contenenti dati sono posti all'interno di locali chiusi Contratto con ditta di manutenzione	DI CONTRASTO / DI CONTENIMENTO DELL'EVENTO DANNOSO	TITOLARE / D.P.O./ INCARICATO MANUTENZ

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	30 di 47

UTILIZZO DI SISTEMI DI VIGILANZA CON TELECAMERE:

Al fine di mitigare ulteriormente il rischio di perdita dati da furto e atti vandalici e allo stesso tempo tutelare la sicurezza delle persone e dei beni aziendali, è stato installato apposito sistema di vigilanza con telecamere così regolamentato:

Burlandi Franco S.r.l., in qualità di Titolare del trattamento, desidera informarLa che, ai sensi dell'art. 13 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali – per ragioni di prevenzione, sicurezza organizzativa, tutela del patrimonio – alcuni locali/spazi esterni nelle varie sedi lavorative – debitamente segnalati tramite la cartellonistica richiesta dal Garante per la Protezione dei Dati Personali – sono presidiati da un sistema di video-sorveglianza.

TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento è Burlandi Franco S.r.l., in persona del legale rappresentante pro-tempore.

DATA PROTECTION OFFICER

In ragione delle attività di trattamento svolte all'interno della Burlandi Franco S.r.l., il Titolare del trattamento ha ritenuto necessario designare, ai sensi dell'art. 37 del Regolamento Europeo, un Data Protection Officer. Per contattare il Data Protection Officer potrà scrivere a Burlandi Franco S.r.l. presso la sede legale o inviare una e-mail all'indirizzo di seguito specificato.

FINALITÀ DEL TRATTAMENTO

Le immagini, al pari del nome, dei dati anagrafici, sono dati personali sottoposti alle tutele previste dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche. Pertanto tali particolari dati personali vengono acquisiti e conservati da Burlandi Franco Srl per il tempo strettamente necessario al fine di prevenire la commissione di attività illecite, di assicurare la sicurezza dei siti, di consentire tutela del patrimonio aziendale, il tutto nel rispetto delle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio e delle prescrizioni imposte dall'Ufficio del Garante per il Trattamento dei dati personali. Il sistema adottato non effettua il collegamento, l'incrocio o il confronto delle immagini raccolte con altri dati personali o con eventuali codici identificativi.

PERIODO DI CONSERVAZIONE DEI DATI PERSONALI

Il Titolare del trattamento procede alla conservazione delle immagini derivanti dall'attività di videosorveglianza per un arco di tempo non superiore rispetto a quello necessario per il conseguimento delle finalità per i quali sono trattati, infatti Burlandi Franco S.r.l. provvede alla distruzione dei dati raccolti entro il termine di **120 ore**, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'Autorità Giudiziaria o di Polizia Giudiziaria. Solo in alcuni casi, per peculiari esigenze e/o in caso del verificarsi di particolari accadimenti, Burlandi Franco S.r.l. potrà estendere la conservazione dei dati predetti per un periodo non superiore ai 7 giorni, salvo l'ipotesi di richiesta da parte dell'Autorità Giudiziaria e/o di Polizia Giudiziaria. Non è previsto l'utilizzo delle immagini per altre finalità ed in particolar modo è esclusa la finalità di controllo a distanza dell'attività lavorativa.

Rev. 1 del 22/09/2020	Emesso da: Arnaldo Basilico	Approvato da: Fabrizio Burlandi
-----------------------	-----------------------------	---------------------------------

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	31 di 47

CATEGORIE DI SOGGETTI DESTINATARI DEI DATI

I dati trattati non saranno oggetto di diffusione a terzi. Possono comunque venire a conoscenza dei Suoi dati, in relazione alle finalità di trattamento precedentemente esposte:

- soggetti che possono accedere ai dati in forza di disposizione di Legge previste dal diritto dell’Unione Europea o da quello dello Stato membro cui è soggetto il Titolare del trattamento;
- il nostro personale dipendente, purché sia precedentemente designato come soggetto che agisce sotto l’autorità del Titolare del trattamento, a norma dell’art. 29 del Regolamento Europeo, o come Amministratore di Sistema;
- soggetti (società di guardiania e vigilanza) che svolgono, all’interno dei confini dell’Unione Europea, in qualità di Responsabili del trattamento all’uopo nominati da Burlandi Franco S.r.l., finalità ausiliarie alle attività e ai servizi.

TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI

Il Titolare del trattamento non intende trasferire i Suoi dati personali verso Paesi terzi. L’intero trattamento dei dati personali, infatti, si svolge all’interno dei confini del territorio italiano, oppure in alcuni e limitati casi entro quelli dell’Unione Europea.

DIRITTI DELL’INTERESSATO

In relazione al trattamento dei Suoi dati personali, ai sensi del Regolamento Europeo, Ella in qualità di interessato ha il diritto di:

revocare il Suo consenso al trattamento in qualsiasi momento. Occorre evidenziare, tuttavia, che la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca, così come previsto dall’art. 7, comma 3, del Regolamento Europeo;

chiedere al Titolare del trattamento l’accesso ai Suoi dati personali, così come previsto dall’art. 15 del Regolamento Europeo;

ottenere dal Titolare del trattamento la rettifica e l’integrazione dei Suoi dati personali ritenuti inesatti, anche fornendo una semplice dichiarazione integrativa, così come previsto dall’art. 16 del Regolamento Europeo;

ottenere dal Titolare del trattamento la cancellazione dei Suoi dati personali qualora sussista anche solo uno dei motivi previsti dall’art. 17 del Regolamento Europeo;

ottenere dal Titolare del trattamento la limitazione del trattamento dei Suoi dati personali qualora ricorrano una delle ipotesi previste dall’art. 18 del Regolamento Europeo;

ricevere dal Titolare del trattamento i dati personali che La riguardano in un formato strutturato, di uso comune e leggibile da dispositivo automatico, nonché ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti, così come previsto dall’art. 20 del Regolamento Europeo;

opporsi in qualsiasi momento, per motivi connessi alla Sua situazione particolare, al trattamento dei Suoi dati personali svolto ai sensi dell’art. 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni, così come previsto dall’art. 21 del Regolamento Europeo;

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	32 di 47

non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, che producano effetti giuridici che La riguardino o che incidano significativamente sulla Sua persona, qualora non abbia preventivamente ed esplicitamente acconsentito, così come previsto dall'art. 22 del Regolamento Europeo. A mero titolo esemplificativo e non esaustivo, rientra in questa categoria qualsiasi forma di trattamento automatizzato di dati personali teso ad analizzare o prevedere aspetti riguardanti le scelte di consumo e di acquisto, la situazione economica, gli interessi, l'affidabilità, il comportamento;

proporre reclamo ad un'autorità di controllo, qualora ritenga che il trattamento che La riguarda violi il Regolamento Europeo. Il reclamo può essere proposto nello Stato membro in cui risiede abitualmente, lavora oppure nel luogo ove si è verificata la presunta violazione, così come previsto dall'art. 77 del Regolamento Europeo.

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	33 di 47

5 Procedura di formazione, scadenziario e notifica al garante

Al D.P.O. è affidato il compito di verificare entro il 31 ottobre di ogni anno le necessità di formazione del personale incaricato di eseguire i compiti indicati nella lettera di incarico. Per ogni incaricato del trattamento il D.P.O. definisce, sulla base dell'esperienza e delle sue conoscenze ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessaria una formazione tecnica adeguata e ne fa immediatamente richiesta al Titolare.

PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI	
Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessate
CORSO DI FORMAZIONE PER SOGGETTI DEL TRATTAMENTO Oggetto: - Informazione sul contenuto e disposizioni della norma UE 2016/679 - Uso delle CREDENZIALI DI ACCESSO ALLA RETE - Concetti di “IGIENE INFORMATICA” - Rilevanza legale del BACK-UP - Il Documento sulla privacy - Natura giuridica della “LETTERA DI NOMINA” - Analisi dei rischi collegati alle attività proprie della categoria - Organizzazione	TITOLARE DEL TRATTAMENTO RESPONSABILE AMMINISTRATIVO DELLE VARIE SEDI RESPONSABILI TRATTAMENTO DELLE VARIE SEDI

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	34 di 47

6 Responsabilità

Il presente Documento è stato redatto sulla base delle informazioni acquisite in uno o più colloqui intercorsi con il personale incaricato dal titolare del trattamento dei dati, a descrivere l'attività svolta negli uffici.

In caso di DATA BREACH / VIOLAZIONE DATI:

In eventuali casi di violazione dei dati personali consistenti nella 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 e tali da mettere a rischio i diritti e le libertà degli individui i cui dati personali sono trattati dal Responsabile, esso deve:

- informare il Titolare del trattamento dei dati tempestivamente ed in ogni caso al massimo entro e non oltre 24 ore dalla scoperta dell'evento, di essere venuto a conoscenza di una violazione e fornire tutti dettagli completi della violazione subita: in particolare, fornendo una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali e sugli interessati coinvolti e le misure adottate per mitigare i rischi;

- fornire assistenza alla Burlandi Franco S.r.l. per far fronte alla violazione e alle sue conseguenze soprattutto in capo agli interessati coinvolti.

Il Responsabile si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive al Titolare del trattamento ed attuando tempestivamente tutte le azioni correttive approvate e/o richieste dalla Burlandi Franco S.r.l.

Il titolare a sua volta dovrà comunicare al diretto interessato la violazione dei dati personali immediatamente.

Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al Trattamento eseguito.

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	35 di 47

7 Documentazione allegata

Vanno allegati al presente documento:

- Allegato I - Piano degli interventi
- Allegato II - Registro comunicazioni violazione dati
- Allegati III – Tracciamento dati
- Allegato IV – Informativa dipendenti
- Allegato V – Schede informazione personale
- Allegato VI – violazione dati / data breach
- Allegato VII – Lettera di nomina per il trattamento dati dipendenti
- Allegato VIII – Lettera di nomina per il trattamento dati aziende e professionisti esterni
- Allegato IX – Lettera di nomina per il D.P.O.

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	36 di 47

8 . Certificazione e sottoscrizione

Il datore di lavoro dichiara di aver messo in atto un piano di autocontrollo in cui sono descritti i pericoli per la privacy e le relative MISURE PREVENTIVE che la Ditta mette in atto per prevenire o tenere sotto controllo tali pericoli: essere a conoscenza e applicare le procedure adottate è un dovere e un obbligo per ciascun operatore.

Il presente documento, è composto di n 47 pagine .

Il Responsabile del trattamento dati

Addetti al trattamento dati personali

Il datore di lavoro

Revisione: 1
22.09.2020

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	37 di 47

ALLEGATO I:

Tabella di riferimento per il piano degli interventi periodici:

<i>RIFERIMENTO</i>	<i>FREQUENZA STABILITA</i>	<i>DOCUMENTI / REGISTRI ALLEGATI</i>
CONTROLLO DOCUMENTAZIONE	UNA VOLTA ANNO	REGISTRO CONTROLLI
VERIFICA DEL CORRETTO RISPETTO DELLA NORMATIVA	UNA VOLTA ANNO	REGISTRO CONTROLLI
ELIMINAZIONE DELLA DOCUMENTAZIONE FISCALE E NON	ALLA SCADENZA DEI DIECI ANNI	REGISTRO CONTROLLI
FORMAZIONE	UNA TANTUM SECONDO REG. UE	ATTESTATO DI FREQUENZA
INCONTRI DI VERIFICA E REVISIONE	ANNUALE	VERBALI
ELIMINAZIONE COPIE DOCUMENTI DI IDENTITA' CLIENTI	ANNUALE	REGISTRO CONTROLLI

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	38 di 47

ALLEGATO II:

REGISTRAZIONE COMUNICAZIONE DATA BREACH DIRETTO INTERESSATO

Data	Che problema c'è stato?	Nominativo responsabile del trattamento	Conseguenze della violazione dei dati	Misure adottate per minimizzare i possibili effetti negativi

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	40 di 47

ALLEGATO IV:

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	42 di 47

ALLEGATO VI:

SCHEDA DI COMUNICAZIONE / DATA BREACH / VIOLAZIONI DATI:

N°	Data	DESCRIZIONE NON CONFORMITA' / DATA BREACH / VIOLAZIONI DATI

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	43 di 47

ALLEGATO VII:

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	44 di 47

ALLEGATO VIII:

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	45 di 47

ALLEGATO IX:

**Alla cortese attenzione Del/della
Signor/a _____**

La Burlandi Franco Srl, con sede legale a Roma in Via di Passo Lombardo 259, Codice Fiscale e P. IVA n° 04571101007, Titolare del trattamento dei dati personali, in persona del legale rappresentante pro tempore,

PREMESSO CHE

- il Regolamento UE 2016/679 o c.d. “GDPR” (General Data Protection Regulation) stabilisce che il Titolare del trattamento dei dati determina le finalità e i mezzi del trattamento di dati personali;
- che ai sensi dell'art. 29 del GDPR il Responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del Titolare del trattamento, che abbia accesso a dati personali, non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento;
- che ai sensi dell'art. 4 n°10 del GDPR, sono autorizzati al trattamento le persone che trattano i dati sotto l'autorità diretta del Titolare o del Responsabile del trattamento;
- il Reg. UE 2016/679 definisce come:

a) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (cfr art. 4 n° 2 GDPR);

b) «**dati personali**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona che può essere identificata direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (cfr art. 4 n°1 GDPR);

c) «**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 (cfr art. 4 n°13 GDPR);

d) «**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 (cfr art. 4 n°14 GDPR);

e) «**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 (cfr art. 4 n°15 GDPR);

- che Burlandi Franco S.r.l., in qualità di “Titolare del trattamento”, intende pertanto procedere alla nomina, ai sensi dell'art. 29 del GDPR, del personale dipendente che nell'adempimento delle mansioni assegnategli effettua operazioni di trattamento sui dati personali.

TUTTO CIO' PREMESSO NOMINA D.P.O.

Il Signor Basilico Arnaldo, nato a Palermo il 05/07/1995, "D.P.O." del trattamento dei dati personali indicati. L'incaricato dovrà verificare che il trattamento dei dati venga effettuato nel rispetto della normativa vigente in materia di protezione dei dati personali e delle misure di sicurezza individuate dal Titolare del trattamento, nonché in conformità dell'ulteriore normativa che dovesse trovare applicazione.

Rev. 1 del 22/09/2020	Emesso da: Arnaldo Basilico	Approvato da: Fabrizio Burlandi
-----------------------	-----------------------------	---------------------------------

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	46 di 47

L'incaricato dovrà, inoltre, lavorare in autonomia dal Titolare del trattamento.

In particolare dovrà controllare:

- raccolta e registro dei dati personali unicamente per finalità inerenti all'attività svolta;
- verificare costantemente i dati ed il loro aggiornamento nonché la completezza e pertinenza dei dati trattati;
- trattamento dei dati personali nella misura necessaria e sufficiente alle finalità proprie della mansione assegnatagli;
- adozione, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate, oggi o in futuro, dal Titolare del trattamento e, in particolare, dovrà vigilare:

a) quando appositamente autorizzato all'accesso alle banche dati informatiche, custodire con attenzione le proprie credenziali di autenticazione ed ogni dispositivo che le contiene ed evitare di operare su terminali altrui e/o di lasciare accessibile il sistema operativo in caso di allontanamento, anche temporaneo, dal posto di lavoro, al fine di evitare trattamenti non autorizzati;

b) trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare;

c) conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che siano accessibili a persone non autorizzate al trattamento dei dati medesimi o siano facilmente oggetto di danneggiamenti intenzionali o accidentali;

d) con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;

e) copie di dati personali oggetto di trattamento devono essere effettuate esclusivamente se necessario e soltanto previa autorizzazione del Titolare del trattamento;

f) in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al Titolare del trattamento;

- segnalare al Titolare del trattamento eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

- mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso. In particolare grava sulla persona autorizzata al trattamento:

a) il divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del Titolare del trattamento;

b) l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;

c) la fase di raccolta del consenso dovrà essere preceduta dalla informativa ed dal consenso al trattamento degli interessati rilasciato in forma scritta.

- svolgere, in ogni caso, il trattamento dei dati personali per le finalità e secondo le modalità stabilite, anche in futuro, dal Titolare del trattamento e, comunque, in modo lecito e secondo correttezza;

- fornire al Titolare del trattamento, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentirgli di svolgere efficacemente la propria attività di controllo;

- osservare le specifiche ulteriori misure di sicurezza riportate nelle Linea guida sull'uso delle risorse informatiche del Titolare del trattamento;

- in generale, prestare la più ampia e completa collaborazione al Titolare del trattamento al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

L'incaricato prende atto che opererà sotto la diretta autorità del Titolare del trattamento che avrà facoltà di revocare in ogni momento il presente incarico.

Le revoche, comunicate in forma scritta, avranno effetto immediato senza obbligo di preavviso. L'incaricato apponendo la sottoscrizione al presente atto ne accetta integralmente il contenuto, assumendo la qualifica di persona autorizzata al trattamento dei dati personali ai sensi dell'art. 29 del Reg.UE 2016/679.

Burlandi Franco S.r.l.	MANUALE DI GESTIONE DELLA PRIVACY – P.I.A. REGOLAMENTO (UE) 2016/679	Data emissione	22.09.2020
		Numero revisione	1
SERVIZIO PREVENZIONE e PROTEZIONE		Numero pagina	47 di 47

Titolare del trattamento

Per integrale accettazione e assunzione della qualifica di D.P.O. _____

Persona autorizzata al trattamento
