MODELLO ORGANIZZATIVO
IN
MATERIA DI PROTEZIONE DEI DATI PERSONALI

Ai sensi del Regolamento Europeo n. 679/2016 (GDPR)

Titolare del trattamento: **Consorzio Campolattaro S.c.a.r.l.**

Sede legale: Via Pietro Borsieri, 2/A – 00195 Roma (RM)
Sede Unità Operativa: Contrada Collepiano, 18/scala 5, 82030 Collepiano l.p. BN
P.IVA 17327891002- info@campolattaroscarl.com

SOMMARIO

PREMESSA

Il Regolamento Europeo n. 2016/679, cosiddetto "General Data Protection Regulation", (di seguito brevemente "GDPR"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi e adempimenti a carico dei soggetti che trattano dati personali.

Il GDPR affronta il tema della tutela dei dati personali attraverso un approccio nuovo, basato principalmente sulla valutazione dei rischi riguardanti i diritti e le libertà degli interessati.

A tale riguardo, l'art. 24 e seguenti del GDPR prevede che il Titolare del trattamento adotti misure tecniche ed organizzative adeguate ed efficaci al fine di garantire che il trattamento dei Dati personali abbia luogo in conformità alle Leggi sulla protezione dei dati applicabili.

Le politiche interne e le misure da attuare per soddisfare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di *default*, devono tener conto, in concreto, della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento nonché del rischio per i diritti e le libertà delle persone fisiche.

L'adeguamento ai requisiti previsti dal GDPR comprende, tra le altre attività di privacy compliance, l'adozione e l'efficace ed effettiva attuazione di un "Modello Organizzativo in Materia di Protezione dei Dati Personali" (di seguito anche "Modello Organizzativo Privacy" o "MOP") che consenta alle imprese, enti ed organizzazioni, cui si applica il Regolamento, di:

a) predisporre un sistema di controllo idoneo a prevenire i rischi privacy relativi ai dati personali e successivamente valutare i controlli esistenti, in termini di adeguatezza ai requisiti previsti dal GDPR ed effettiva operatività degli stessi;
b) gestire tempestivamente possibili criticità;

c) dare evidenza del sistema di controllo implementato evitando l'imputazione di responsabilità e delle sanzioni previste.

Pertanto, il Consorzio Campolattaro S.C.A.R.L. (in seguito anche ""Campolattaro" o "Consorzio"), al fine di rispettare i principi fissati dal Regolamento, ha voluto elaborare il presente Modello Organizzativo della Privacy (nel seguito anche il "MOP" o "Modello"), che ha richiesto la preventiva esecuzione di una attenta e critica attività di *auditing* interno, la quale ha consentito l'esame di ogni singola realtà aziendale e della valutazione d'impatto sulla protezione dei dati personali.

Il presente Modello, infatti, raccoglie le misure tecniche ed organizzative che la Società attua per garantire - ed essere in grado di dimostrare - la conformità al Regolamento UE 2016/679 delle attività di trattamento dei dati personali delle persone fisiche, Cittadini Europei e residenti nell'Unione Europea, che il Consorzio effettui direttamente o che soggetti terzi effettuino per suo conto.

DEFINIZIONI

Ai fini della seguente Policy, i termini e le espressioni definite avranno il significato nel seguito indicato. Le espressioni al singolare manterranno lo stesso significato al plurale, ove il contesto lo richieda. Si riportano nel seguito le definizioni rilevanti ai fini della presente Procedura:

- Archivio: indica qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- Atto di Nomina o Nomina: indica l'atto di nomina di volta in volta adottato dal Titolare volto a regolamentare il Trattamento dei dati personali effettuato da parte dei Responsabili del trattamento. Tale Nomina costituisce parte integrante e

sostanziale della presente Policy.

- Autorità: indica l'Autorità Garante per la Protezione dei Dati personali.
- Autorizzati: indica i dipendenti della Società autorizzati dal Titolare a compiere operazioni di trattamento nell'esercizio delle funzioni agli stessi affidate.
- Cancellazione dei Dati: indica la distruzione definitiva – fisica o tecnica – idonea a rendere non più recuperabili mediante gli ordinari mezzi disponibili in commercio le informazioni contenute in un supporto elettronico e/o cartaceo.
- Consenso dell'Interessato: indica 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.
- Data Breach: indica una 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 oggetto di trattamento.
- Data Breach Policy: indica la Procedura adottata dalla Società al fine di disciplinare le opportune modalità di gestione del Data Breach.
- Data Manager: indica i dipendenti designati direttamente dal Titolare che, nello svolgimento delle proprie funzioni e nei limiti dei poteri loro attribuiti, sono deputati alla gestione e al monitoraggio dei Trattamenti effettuati nell'ambito della propria attività.
- Dati Biometrici: indica i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

- Dati Genetici: indica i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- Dati Giudiziari: dati personali relativi alle condanne penali e ai reati o connesse a misure di sicurezza (giurisdizione penale).
- Dati Personali: 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 o cognome,
  - indirizzo e-mail,
  - immagine e voce,
  - un numero di identificazione (Carta d'Identità, Codice Fiscale, Passaporto ecc.),
  - dati relativi all'ubicazione.
- 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;
- Destinatari: indica gli amministratori, i dirigenti, i dipendenti, i collaboratori, i Responsabili del trattamento dei dati, i fornitori e i soggetti terzi che effettuano operazioni di trattamento dei dati di cui la Società è Titolare e nei confronti dei quali trova applicazione la presente Policy e le relative procedure che formano parte integrante della stessa;
- GDPR: indica il Regolamento Generale sulla protezione dei dati n. 2016/679.

- Informativa: documento con il quale vengono fornite all'Interessato le seguenti informazioni:
  - l'identità e i dati di contatto del titolare del trattamento;
  - i dati di contatto del responsabile della protezione dei dati;
  - le finalità del trattamento;
  - gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
  - l'intenzione del Titolare del trattamento di trasferire dati personali a un Paese terzo o a un'Organizzazione internazionale;
  - il periodo di conservazione dei dati personali;
  - i diritti dell'interessato (15-22 GDPR)
  - il diritto di proporre reclamo a un'Autorità di controllo (Garante per la protezione dei dati personali)
  - la base giuridica del trattamento
  - l'esistenza di un processo decisionale automatizzato, compresa la profilazione.
- Incaricato: indica le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- Interessato: indica la persona fisica a cui si riferiscono i Dati Personali oggetto di trattamento;
- Leggi sulla protezione dei dati: indica tutte le leggi e i regolamenti, inclusi ma non limitati al Regolamento (UE) 2016/679, in materia di protezione delle persone fisiche con riguardo al Trattamento dei Dati personali, nonché alla libera circolazione dei dati (GDPR) e al Codice in materia di Protezione dei Dati Personali ex D.lgs. 196/2003 e successive modifiche (Codice Privacy) nonché provvedimenti di volta in volta in vigore che sono applicabili al Trattamento dei Dati personali;

- Policy Privacy: indica la presente Policy organizzativa adottato dal Consorzio al fine di garantire la corretta gestione e implementazione dei presidi previsti dalle Leggi sulla protezione dei dati. Costituiscono parte integrante e sostanziale della presente Policy, le Procedure e il Registro dei Trattamenti;
- Paese Terzo: indica un Paese esterno allo Spazio Economico Europeo;
- Privacy Officer: indica la funzione individuata dal Titolare che sovraintende all'implementazione e all'aggiornamento dei presidi previsti dalle Leggi sulla protezione dei dati;
- Procedura: Si indicano le policy e procedure adottate dal Consorzio. al fine di regolamentare i diversi aspetti legati al trattamento dei Dati personali. A mero titolo esemplificativo, rientrano nella definizione di Procedura:
    - Procedura per l'esercizio dei diritti degli Interessati: indica la procedura adottata dal Titolare al fine di disciplinare le azioni da compiere da parte dei soggetti coinvolti nelle operazioni di Trattamento di Dati personali di cui la Società è Titolare al fine di agevolare e garantire l'esercizio dei Diritti degli Interessati;
    - Procedura sulla conservazione dei Dati Personali o Data Retention Policy: indica la procedura volta a illustrare le linee guida che il Consorzio ha inteso adottare in materia di conservazione dei Dati personali e garantire tali prescrizioni, nonché le misure di sicurezza. Tale procedura individua, infine, il rispetto dei diritti di cancellazione dei Dati personali esercitati dagli Interessati;
- Profilazione: indica 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;

- Registro dei Trattamenti: indica il presidio che la Società, ai sensi dell'art. 30 GDPR, ha implementato al fine di mappare le operazioni di trattamento dei Dati personali di cui è Titolare del trattamento dei dati;
- Responsabile del trattamento dei Dati (Data Processor): indica l'entità esterna alla Società che tratta Dati personali per conto del Titolare del trattamento dei dati;
- Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

  Trattamento: indica 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;
- WP29: indica il Gruppo Articolo 29 ossia un organismo consultivo indipendente composto da un rappresentante delle varie autorità nazionali, dal Garante Europeo della protezione dei dati, nonché da un rappresentante della Commissione Europea.

1.1.I PRINCIPI GENERALI E LE NUOVE REGOLE PER IL TRATTAMENTO DEI DATI PERSONALI

Il GDPR è costituito da tre principi ispiratori, che sostengono l'intero impianto normativo ed il cui rispetto è protetto da un sistema sanzionatorio, delineato dagli artt. 83 e ss., caratterizzato dalle rilevanti cifre che arrivano a colpire Titolari e Responsabili del trattamento con sanzioni amministrative fino a 20 milioni di euro o fino al 4 % del fatturato mondiale totale annuo, cui si aggiungono le sanzioni penali previste dalla normativa nazionale.

Tali principi essenziali sono:

- il principio di Accountability o di Responsabilizzazione, sulla base del quale tutti i dati devono essere trattati dal Titolare in modo responsabilizzato. Il Titolare deve quindi dimostrare, per ciascun Trattamento, di aver agito in conformità alle disposizioni del GDPR. L'approccio metodologico da applicarsi al fine di garantire l'Accountability è un approccio "risk based", ovvero un approccio basato sulla valutazione del rischio del Trattamento, che deve essere adottato e dimostrato da parte delle imprese, degli enti o delle organizzazioni. E' un tipo di approccio proattivo, e non più reattivo, con focus su obblighi e comportamenti finalizzati a prevenire in modo effettivo il possibile evento di danno. Il rischio inerente al Trattamento è da intendersi come rischio per la sicurezza dei dati e come rischio di impatti negativi sulle libertà e i diritti degli interessati. Tali impatti devono essere analizzati attraverso un apposito processo di valutazione (es. Risk e Privacy Impact Assessment) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) da adottare per mitigare tali rischi. L'approccio metodologico "risk based" deve quindi seguire logiche di risk assessment e risk management, al fine di valutare e ridurre il rischio per i diritti e le libertà dei soggetti dei dati e individuare le misure tecniche e organizzative idonee a garantire un adeguato livello di sicurezza;

- Privacy by Default, che implica l'implementazione da parte dell'organizzazione di un processo che preveda e disciplini le modalità di acquisizione, trattamento, protezione e modalità di diffusione dei dati personali, limitando la raccolta dei dati esclusivamente a quei dati personali realmente necessari per la realizzazione delle finalità perseguite, in ottemperanza al principio di minimizzazione dei dati, e determinando sin dall'origine il periodo per il quale i dati personali raccolti dovranno essere conservati;
- Principi ispiratori di base che si riflettono sui cosiddetti "pilastri" del GDPR, ossia sulle principali novità operative quali:
  a) l'istituzione del Registro delle Attività di Trattamento (art.30 e cons. 171) che costituisce il punto di partenza per la predisposizione dell'intero impianto documentale, deputato a raccogliere le evidenze, i controlli ed i processi che consentono di soddisfare l'accountability del sistema privacy;
  b) Il Processo di Data Breach, (art. 33 e 34), ossia la notifica delle eventuali violazioni dei dati personali, che richiede un'attenta analisi e conoscenza delle informazioni gestite, ma soprattutto investimenti tecnologici nelle modalità di monitoraggio, securizzazione e compartimentazione dei danni che ne possono derivare. Nei casi di violazione dei dati, accesso abusivo o, comunque, perdita degli stessi, i Titolari dei trattamenti saranno obbligati, entro 72 ore, ad avvisare l'Autorità di Controllo e, nei casi di particolare gravità, anche i diretti interessati, informando in relazione alle possibili conseguenze, alle misure adottate per rimediare o ridurre l'impatto del danno e ai dati di contatto degli organi e delle figure aziendali che vigilano sulla gestione e protezione del trattamento di dati personali in conformità alla legge.

Diretto corollario dei sopra riferiti principi generali di Accountability, Privacy by Design e Privacy by Default, è che la piena compliance al GDPR impone che il trattamento dei dati personali avvenga secondo i principi di LICEITA', CORRETTEZZA e TRASPARENZA.

Il trattamento è LECITO allorché trovi fondamento in una base giuridica che, fermo restando in ogni caso l'obbligo di informativa a carico del Titolare del trattamento, può consistere in quanto segue:

1. Consenso dell'interessato che deve essere libero, specifico, informato ed inequivocabile, non essendo ammesso il consenso tacito o presunto: deve, in altri termini, essere manifestato attraverso una "dichiarazione o azione positiva inequivocabile". Inoltre per i dati "sensibili" di cui all'art. 9, esso deve essere anche "esplicito", non necessariamente "documentato per iscritto" né da prestare in "forma scritta", sebbene tale modalità sia quella maggiormente idonea a dimostrare la sua prestazione, la sua inequivocabilità ed il suo essere "esplicito". Il consenso deve essere esplicitamente prestato per ogni trattamento effettuato, ove non operino le esenzioni di legge. A tal proposito, se la richiesta per ottenere il consenso dagli interessati viene inserita nell'ambito di altre dichiarazioni essa va distinta e formulata con linguaggio semplice e chiaro. Condizione di validità del consenso è che le finalità per cui viene richiesto siano esplicite, legittime, adeguate e pertinenti. Nel caso in cui il consenso al trattamento dei dati personali per una o più specifiche finalità riguardi i minori, il GDPR richiede al Titolare del Trattamento la verifica documentata dell'età del minore e, laddove necessario sulla base dell'età del minore, del consenso al trattamento da parte di un genitore o da chi eserciti la responsabilità genitoriale. I Titolari del Trattamento dei dati devono essere

in grado di dimostrare che l'interessato abbia prestato il consenso e il consenso possa essere ritirato o modificato;

2. adempimento di obblighi contrattuali, ossia il trattamento è lecito se è necessario all'esecuzione di un contratto di cui l'interessato è parte od all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
3. obblighi di legge cui è soggetto il titolare del trattamento, nel qual caso la finalità è specificata per legge;
4. interessi vitali della persona interessata o di terzi: ossia se è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; utilizzabile però come base giuridica solo se nessuna delle altre condizioni di liceità può trovare concreta applicazione;
5. legittimo interesse prevalente del titolare o di terzi cui i dati vengono comunicati, ossia quando il trattamento è necessario per il perseguimento dei legittimi interessi del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore;
6. interesse pubblico o esercizio di pubblici poteri, ovvero necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del Trattamento (tramite legge statale o dell'Unione) ed anche in tal caso la finalità deve essere specificata per legge.

Il trattamento dei dati personali è CORRETTO se trasparente nei confronti degli interessati, ossia

i dati personali devono essere trattati per scopi determinati, espliciti e legittimi, e senza scorrettezze o raggiri nei confronti degli interessati (essendo dunque vietata un'informazione confusa o parziale).

Quello della TRASPARENZA non è solo un principio fondamentale del trattamento, ma anche un vero e proprio diritto dell'interessato: devono cioè essere trasparenti e corrette le modalità di raccolta dei dati e di utilizzo degli stessi. Gli interessati devono essere informati in merito alle finalità del trattamento, alle modalità del trattamento e all'indirizzo del titolare del trattamento, prima che si avvii il trattamento stesso. Le modalità del trattamento devono essere esplicitate in maniera comprensibile in modo che gli interessati siano in grado di capire cosa accadrà ai loro dati. L'interessato deve avere a disposizione una procedura efficace e accessibile per consentirgli di ottenere l'accesso ai suoi dati in un tempo ragionevole, e quindi di conoscere se e quali dati sono detenuti dal titolare. Qualsiasi trattamento occulto o segreto deve, quindi, ritenersi illecito. I titolari e i responsabili devono garantire agli interessati che i dati saranno trattati secondo liceità e correttezza e in modo da conformarsi, per quanto possibile, alla volontà degli stessi interessati.

2. OBIETTIVO E STRUTTURA DEL MODELLO

Il presente documento costituisce il Modello Organizzativo Privacy del Consorzio che effettua trattamenti di Dati, nella sua qualità di Titolare e/o di Responsabile.

L'obiettivo del Modello è quello di garantire e dimostrare che il trattamento dei dati personali da parte del Consorzio avviene in modo lecito, corretto e trasparente, secondo i parametri giuridici individuati dal GDPR, raggiungibile attraverso la realizzazione di una gestione interna organizzata e strutturata.

Il Consorzio promuove nei propri collaboratori una cultura della privacy e della tutela e

sicurezza dei dati personali, consolidando quei principi comportamentali idonei a garantire la trasparenza, la sicurezza e la correttezza dei trattamenti effettuati, aumentando la propria affidabilità verso i propri clienti, partners strategici, dipendenti ed interessati.

Il MOP descrive le attività poste in essere dalla Società per assicurare la conformità al GDPR e il relativo approccio metodologico utilizzato, oltre agli aspetti di governance, risk management e compliance applicabili alla protezione dei dati personali con la finalità di definire:

i. i meccanismi organizzativi e gestionali, inclusi ruoli, responsabilità in materia di protezione dei dati personali ("governance");
ii. le modalità di gestione dei rischi in materia di protezione dei dati personali ("risk management");
iii. un sistema strutturato di procedure a presidio dei rischi che sono stati rilevati, nonché una costante azione di monitoraggio sulla corretta attuazione di tale sistema in conformità ai requisiti normativi applicabili in materia di protezione dei dati personali ("compliance").

Il Consorzio consapevole dell'importanza di adottare ed efficacemente attuare un Modello Organizzativo Privacy, ha predisposto questo documento, che costituisce un valido strumento di sensibilizzazione dei destinatari per assumere comportamenti conformi ai requisiti del GDPR.

Il Modello si compone di n.12 Sezioni dirette a fornire una panoramica sul sistema complessivo delle misure tecniche e organizzative che, sulla base delle concrete esigenze sistematiche ed operative della Società, si ritengono adeguate, contenendo i principi, le regole organizzative e gli strumenti di controllo per garantire il trattamento lecito, corretto e trasparente dei dati personali. Il MOP mira infatti, a rafforzare l'etica sul lavoro che contraddistingue il Personale che collabora con la Società.

Per il Consorzio è fattore di competitività poter ambire ad una corretta gestione del dato

personale durante lo svolgimento del proprio operato. Il presente modello infatti ha lo scopo di evitare la possibile erogazione di sanzioni amministrative pecuniarie di cui all'art. 83 GDPR nonché di quelle penali di cui alla normativa nazionale potendo, con la sua adozione, dimostrare l'attuazione concreta, efficiente ed efficace delle misure tecniche e organizzative adeguate alla protezione dei dati personali da essa trattati, direttamente o tramite soggetti terzi che li effettuano per suo conto.

3. POLICY AZIENDALE

Il **Consorzio Campolattaro S.c.a.r.l.** si è costituito il 6 ottobre 2023, assumendo come forma giuridica quella della società consortile a responsabilità limitata. Il Consorzio nasce per "volontà" delle società "GHELLA S.P.A.", "TUNNELPRO S.P.A.", "ITINERA S.P.A.", "RDR S.P.A SOCIETÀ BENEFIT" e "IDROAMBIENTE S.R.L.".L'oggetto sociale del Consorzio è prevalentemente consortile, e quindi mutualistico, e riguarda la realizzazione della Progettazione esecutiva e dei lavori e servizi di ingegneria e architettura per l'utilizzo idropotabile delle acque dell'invaso di Campolattaro e potenziamento dell'alimentazione potabile per l'area beneventana, suddiviso in 3 (tre) lotti, numero riferimento 3593 / RI / 2023, CUP B87B 2009 8990 009 di cui i lotti 1 e 2 aggiudicati alle imprese consorziate.

Nello svolgimento di tali attività, Campolattaro S.c.a.r.l. gestisce differenti tipologie di Dati Personali, ovvero:

1. Dati Anagrafici in senso stretto riferibili ai lavoratori ed ai loro familiari, dipendenti propri e delle imprese appaltatrici e sub-appaltatrici, alle persone fisiche costituenti il Management aziendale, ai legali rappresentanti di imprese fornitrici di beni e servizi nonché di professionisti e consulenti esterni;
2. Dati Giudiziari riferibili alle persone fisiche operanti nell'ambito del Consorzio di imprese fornitrici di beni, servizi e lavori quali i legali rappresentanti, i singoli soci, i singoli

componenti degli organi amministrativi e di controllo ed i rispettivi familiari conviventi;

3. Dati relativi alla salute dei lavoratori inquadrati ad ogni livello aziendale;
4. Dati atti a rivelare l'appartenenza sindacale dei lavoratori;
5. Dati Bancari dei lavoratori e dei fornitori;
6. Dati Biometrici, quali le fotografie dei lavoratori dipendenti, dei professionisti e dei consulenti esterni, necessarie all'elaborazione dei tesserini di riconoscimento per l'accesso in sede ed in cantiere nonché del Management aziendale, destinate ad essere pubblicate sul sito internet ufficiale della Società.

La base giuridica del trattamento di tali dati da parte del Consorzio è rappresentata da:

- l'adempimento degli obblighi contrattuali e pre-contrattuali di cui la Società è parte;
- l'adempimento degli obblighi di Legge cui la stessa è tenuta;
- per finalità amministrativo-contabili;
- legittimo interesse del Titolare.

3.1. AMBITO DI APPLICAZIONE

CAMPOLATTARO S.C.A.R.L. adotta un complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, per assicurare un livello idoneo di protezione dei dati personali, sia nel caso di trattamenti con strumenti elettronici, che per trattamenti senza l'ausilio di strumenti elettronici.

Quando gestiti in forma cartacea, tutti i documenti sono custoditi in armadi e/o schedari chiusi a chiave all'interno delle stanze dei relativi Responsabili e/o Incaricati, anch'esse chiuse a chiave. Sono impartite a tutti gli incaricati precise istruzioni sul trattamento dei dati e delle pratiche cartacee, in particolare la duplicazione elettronica mediante scansione dei documenti cartacei, onde prevenirne la distruzione totale accidentale e la pseudonimizzazione mediante

l'archiviazione dei documenti basata sul numero di matricola e/o codici univoci che non consentono l'immediata identificazione della persona dell'interessato, la quale è consentita solo a determinati soggetti, a tal fine autorizzati, cui sono accessibili le tabelle di conversione nome/matricola.

Regolarmente i Responsabili di ciascuna funzione controllano che le regole di tenuta della documentazione cartacea siano osservate da tutti gli incaricati sottoposti.

Quando gestiti in forma elettronica, i dati ed i relativi documenti vengono trattati mediante personal computers portatili, nonché smartphones messi a disposizione del personale ed utilizzati in esclusiva da ciascun incaricato. I dispositivi informatici sono tutti protetti da un doppio ordine di passwords: la prima richiesta all'atto dell'accensione del terminale e la seconda per l'accesso alle piattaforme informatiche gestionali. Entrambe le passwords sono conoscibili esclusivamente dall'affidatario del dispositivo informatico.

In particolare, le piattaforme informatiche aziendali con funzione gestionale in uso sono protette da passwords e differenziate a seconda della Funzione e della posizione gerarchica aziendale in cui si colloca l'incaricato.

A tali piattaforme aziendali hanno accesso il Personale dipendente del Consorzio., le Società, i Professionisti ed i Consulenti esterni dalla stessa nominati ai sensi dell'art. 28 del GDPR, ai quali il Titolare del trattamento ha imposto il rispetto della riservatezza fin dall'atto della nomina, se non già tenuti per legge al rispetto del segreto professionale.

Il Consorzio., si avvale inoltre di *social networks* per scopi divulgativi e informativi e di un proprio sito internet ufficiale, nell'ambito del quale i dati comunicati dall'utenza o comunque raccolti nel corso della navigazione non sono di norma accompagnati da alcuna informazione personale aggiuntiva rispetto agli usuali dati la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet (quali ad esempio nomi di dominio, indirizzi IP, sistema operativo

utilizzato, tipo di device e di browser utilizzati per la connessione) e vengono trattati per gestire esigenze di controllo delle modalità di utilizzo dello stesso, accertare responsabilità in caso di ipotetici reati informatici e ricavare informazioni statistiche anonime sull'uso del sito. La base giuridica che legittima il trattamento di tali dati è la necessità di rendere utilizzabili le funzionalità del sito a seguito dell'accesso dell'utente. Nel caso di invio da parte dell'utenza del sito informatico di curriculum vitae a scopi di recruiting, i dati personali aggiuntivi sono raccolti e trattati esclusivamente per finalità di selezione ed in tal caso la base giuridica che legittima il trattamento è l'esecuzione di misure precontrattuali adottate su richiesta dello stesso candidato. Qualora sia necessario o strumentale per l'esecuzione delle specifiche finalità, i dati personali, oltre che dal personale interno del Consorzio sono comunicati a destinatari nominati ai sensi dell'art. 28 del GDPR, che li trattano in qualità di Responsabili e/o in qualità di persone fisiche che agiscono sotto l'autorità del Titolare e del Responsabile al fine di ottemperare ad obblighi di legge, a contratti o alle finalità connesse.

Precisamente, i dati possono essere comunicati a destinatari appartenenti alle seguenti categorie:

- Società Partners;
- Soggetti che forniscono servizi per la gestione del sistema informativo e delle reti di comunicazione del Consorzio, ivi compresa la posta elettronica;
- Studi professionali o Società nell'ambito di rapporti di assistenza e consulenza;
- Autorità competenti per adempimenti di obblighi di legge e/o di disposizioni di Organi Pubblici, su richiesta;
- Istituti di Credito e Compagnie Assicurative;
- Società Committenti;
- Società di informazione commerciale per la valutazione della solvibilità e delle

abitudini di pagamento e/o a soggetti per finalità di recupero crediti.

L'elenco dei Responsabili del trattamento designati è costantemente aggiornato e disponibile presso la sede di Campolattaro S.c.a.r.l. e sui suoi portali informatici.

La Società garantisce che i dati oggetto di trattamento siano custoditi e controllati anche in relazione alle conoscenze acquisite in base allo stato dell'arte e all'avanzamento tecnologico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee misure di sicurezza, i rischi di distruzione o perdita, anche accidentale , dei dati stessi , di accesso non autorizzato o di trattamento non consentito non conforme alle finalità della raccolta.

Nel rispetto di quanto previsto dall'art. 5, comma 1, lett. e) del GDPR, i dati raccolti vengono conservati in una forma che consenta l'identificazione dell'interessato per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati stessi sono trattati o in base alle scadenze previste dalle norme di legge.

Per conseguire sempre l'allineamento normativo e aumentare la capacità di controllo, il Consorzio ha inteso adottare un approccio prudenziale, rispettoso del GDPR oltre quanto strettamente dovuto attraverso:

- la richiesta del consenso esplicito dell'interessato, anche quando non strettamente necessario;
- l'espletamento della valutazione di impatto, ritenuta opportuna sebbene non obbligatoria;
- la nomina di Responsabili del trattamento "interni", al fine di garantire l'applicazione e la vigilanza capillari circa il rispetto del Regolamento.

4. IL TITOLARE DEL TRATTAMENTO

Secondo l'articolo 4 del GDPR, il titolare del trattamento è 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.

Nel caso di specie il Titolare del trattamento è il Consorzio Campolataro S.c.a.r.l., nella persona del suo legale rappresentante, il Dott. Paolo Bernardini ed alla stessa spetta il compito di adottare le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il Trattamento dei Dati personali sia effettuato conformemente alle Leggi sulla protezione dei dati.

In particolare, il Titolare è chiamato, a titolo esemplificativo e non esaustivo, a:

- adeguare il proprio assetto organizzativo per rendere il governo della privacy allineato ai dettami normativi;
- adottare le modalità operative necessarie alla corretta gestione degli adempimenti ai fini della protezione dei dati personali trattati;
- assumere le decisioni in ordine alle finalità, alle modalità del trattamento dei dati e agli strumenti utilizzati, ivi compreso il profilo della sicurezza, sia per i trattamenti svolti all'interno che all'esterno della propria struttura;
- individuare e designare i Responsabili del trattamento dei dati, impartendo loro le relative direttive e, se necessario, istruzioni specifiche;
- vigilare sulla puntuale osservanza delle disposizioni e istruzioni impartite a tutti i soggetti che hanno un ruolo attivo nel trattamento dei dati personali;
- garantire sempre il pieno controllo sulla piramide organizzativa di cui è al vertice, concedendo autorizzazioni generali o specifiche ai responsabili del trattamento secondo criteri di opportunità nelle diverse situazioni ed esprimendo o negando il gradimento nei confronti di sub-responsabili eventualmente proposti dai

responsabili assumendo così un ruolo di effettivo controllo e indirizzo.

Inoltre, si impegna a garantire l'esercizio dei diritti degli Interessati e a tal scopo individua e mette in pratica apposite procedure al fine di informare gli interessati e garantire a ciascuno di essi almeno il:

- Diritto all'accesso, cioè di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e di averne accesso. In particolare l'interessato ha diritto di conoscere l'origine dei dati personali; le finalità e modalità del trattamento; la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; gli estremi identificativi del titolare, dei responsabili e degli eventuali rappresentanti designati; l'elenco dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza a qualsiasi titolo in linea con la normativa e quello dei soggetti autorizzati al trattamento;
- Diritto alla rettifica, cioè di ottenere l'aggiornamento, la correzione ovvero, quando vi ha interesse, l'integrazione dei dati;
- Diritto alla cancellazione, cioè di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- Diritto all'opposizione, cioè di limitare od opporsi, per motivi legittimi, al trattamento, seguendo le modalità descritte dalle norme vigenti. Al fine di esercitare i diritti sopra descritti, l'ente si impegna a rispondere senza ritardo alle richieste presentate da parte dell'Interessato direttamente ad esso, ai Responsabili o ai soggetti autorizzati appositamente nominati, nelle forme e modalità nonché attraverso i mezzi ritenuti più idonei.

4.1 IL RESPONSABILE DEL TRATTAMENTO

Il Responsabile del Trattamento dei dati è il soggetto, persona fisica o giuridica, nominato dal Titolare al fine di garantire nelle operazioni di trattamento l'attuazione delle misure di sicurezza previste dalla normativa e dal presente Modello Organizzativo Privacy. Il soggetto preposto allo svolgimento della funzione viene individuato tra quelli in possesso dei necessari requisiti e con adeguate garanzie. Tra le sue funzioni sono comprese quelle di:

- osservare le procedure in materia di protezione dei dati personali adottate dal Titolare;
- organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni di legge e predisporre tutti i documenti nonché le misure tecniche organizzative richiesti dal Codice e dal Regolamento;
- adottare e verificare il rispetto delle misure di sicurezza indicate dal Codice e dal Regolamento e la conformità nel tempo dei sistemi e delle misure di sicurezza;
- redigere e aggiornare il Registro delle Attività di Trattamento, qualora sia necessario;
- informare il Titolare del trattamento di tutte le misure adottate e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato al compito specifico;
- nominare i soggetti autorizzati che svolgono tali funzioni per suo conto, conservando i relativi estremi identificativi, definendo gli ambiti di operatività consentiti e verificando almeno annualmente il relativo operato per controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti il

trattamento dei dati personali;

- nominare i soggetti autorizzati al trattamento dei dati nelle altre funzioni ritenute necessarie conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione;
- osservare le procedure in materia di protezione dei dati personali adottate dal Titolare;
- organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni di legge e predisporre tutti i documenti nonché le misure tecniche organizzative richiesti dal Codice e dal Regolamento;
- adottare e verificare il rispetto delle misure di sicurezza indicate dal Codice e dal Regolamento e la conformità nel tempo dei sistemi e delle misure di sicurezza;
- redigere e aggiornare il Registro delle Attività di Trattamento, qualora sia necessario;
- informare il Titolare del trattamento di tutte le misure adottate e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato al compito specifico;
- nominare i soggetti autorizzati che svolgono tali funzioni per suo conto, conservando i relativi estremi identificativi, definendo gli ambiti di operatività consentiti e verificando almeno annualmente il relativo operato per controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti il trattamento dei dati personali;
- nominare i soggetti autorizzati al trattamento dei dati nelle altre funzioni ritenute necessarie conferendo loro apposite istruzioni sulle norme e le procedure da

osservare e provvedendo alla relativa formazione;

- osservare le procedure in materia di protezione dei dati personali adottate dal Titolare;
- organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni di legge e predisporre tutti i documenti nonché le misure tecniche organizzative richiesti dal Codice e dal Regolamento;
- adottare e verificare il rispetto delle misure di sicurezza indicate dal Codice e dal Regolamento e la conformità nel tempo dei sistemi e delle misure di sicurezza;
- redigere e aggiornare il Registro delle Attività di Trattamento, qualora sia necessario;
- informare il Titolare del trattamento di tutte le misure adottate e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato al compito specifico;
- nominare i soggetti autorizzati che svolgono tali funzioni per suo conto, conservando i relativi estremi identificativi, definendo gli ambiti di operatività consentiti e verificando almeno annualmente il relativo operato per controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti il trattamento dei dati personali;
- nominare i soggetti autorizzati al trattamento dei dati nelle altre funzioni ritenute necessarie conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione.

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle

persone fisiche, il Titolare del trattamento può modificare la propria struttura per conseguire i migliori risultati di protezione variando opportunamente l'articolazione del proprio Sistema di Gestione Privacy.

Parimenti, da una parte generale e da una speciale è caratterizzato anche il contratto di nomina dei Responsabili del trattamento "esterni" rispetto all'organico di Campolattaro S.C.A.R.L.., destinato a rivestire la forma di addendum per i contratti già in essere e ad essere integrato all'interno del testo contrattuale per i nuovi affidamenti.

4.2. INCARICATI DEL TRATTAMENTO

Gli incaricati del trattamento di CAMPOLATTARO S.C.A.R.L. sono coloro i quali, facenti parte dell'organico della Società provvedono materialmente al Trattamento dei Dati Personali sotto la supervisione del relativo Responsabile Interno di settore.

Il soggetto autorizzato effettua tutte le operazioni di trattamento dei dati personali attinenti l'attività lavorativa di competenza dell'area di appartenenza e opera sotto l'autorità del Titolare (o del Responsabile del Trattamento), attenendosi alle istruzioni dallo stesso impartite nonché alle specifiche procedure che regolamentano le modalità di utilizzo delle banche dati cui lo stesso abbia accesso. In particolare, i compiti a esso attribuiti sono così sintetizzati:

- segnalare al Titolare del trattamento, eventuali richieste ricevute da parte dell'interessato sull'esercizio dei relativi diritti, nonché attenersi alla procedura interna sull'esercizio dei diritti;
- avvisare il Titolare del trattamento qualora, nello svolgimento di un'attività, dovesse riscontrare il trattamento di nuovi dati e finalità per cui risultasse necessario aggiornare il Registro dei Trattamenti ed eseguire almeno un'analisi dei rischi, in applicazione dei

principi di privacy by design e privacy by default;

- informare immediatamente il Titolare del trattamento qualora le istruzioni ricevute risultino non conformi alla normativa sulla protezione dai dati;
- segnalare al Titolare del trattamento eventuali accessi non autorizzati;
- rilasciare all'interessato l'informativa e acquisire il consenso laddove necessario, secondo le istruzioni impartite dal Titolare del trattamento (o del Responsabile del trattamento di riferimento).

Il Consorzio., infine, cura l'aggiornamento costante dei propri incaricati mediante corsi di formazione ed aggiornamento.

5. FUNZIONI E PROCESSI INTERESSATI

La politica della privacy che discende dal presente Modello Organizzativo Privacy si applica all'azienda nella sua interezza, a tutti gli organi e alla struttura di qualsiasi livello organizzativo e funzionale.

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni trattate nell'espletamento delle procedure aziendali, rispetto alle quali CAMPOLATTARO S.C.A.R.L. ne assicura l'integrità e la protezione e consente l'accesso esclusivamente ai ruoli e alle funzioni necessarie e preventivamente autorizzate.

Pertanto, si illustrano nel dettaglio, per ogni singola funzione, responsabile del Trattamento di dati, le categorie di dati personali trattati dalle singole funzioni:

1. La funzione Acquisti e contrattualistica, Protocollo di legalità gestisce le seguenti categorie di dati personali:
    a) dati anagrafici;

b) dati personali relativi alle condanne penali ed ai possibili reati riguardanti le persone fisiche delle imprese fornitrici di beni e servizi e precisamente dei legali rappresentanti, dei singoli soci, dei singoli componenti degli organi amministrativi e di controllo e dei rispettivi familiari conviventi.

2. La funzione Amministrazione e finanza, Risorse Umane e Servizi Generali gestisce i seguenti dati personali:

a) dati anagrafici in senso stretto, dei legali rappresentanti delle imprese fornitrici di beni e servizi, funzionali alla stipula ed all'esecuzione dei contratti nonché dei lavoratori dipendenti e del loro nucleo famigliare, necessari alla loro identificazione personale ed alla corresponsione degli assegni familiari e delle altre provvidenze di legge, ove dovuti;

b)) i dati relativi alla salute dei lavoratori, funzionali a verificare - preliminarmente all'instaurazione del rapporto di lavoro - l'idoneità del lavoratore alle mansioni cui sarà assegnato e, a rapporto già instaurato, ad assolvere gli obblighi del datore di lavoro CAMPOLATTARO S.C.A.R.L. derivanti dalla legge o dal contratto individuale nonché l'esatto adempimento della prestazione e commisurare l'importo della retribuzione;

c) I dati atti a rivelare l'appartenenza sindacale dei lavoratori, necessari all'esercizio dei diritti sindacali dei lavoratori come per legge;

d) dati bancari dei lavoratori necessari al pagamento delle retribuzioni e delle competenze.

3. L'Ufficio legale gestisce i seguenti dati personali:

a) dati anagrafici in senso stretto dei legali rappresentanti delle imprese fornitrici di beni e servizi, funzionali alla stipula ed all'esecuzione dei contratti;

b) dati personali, anche dei lavoratori, inerenti a procedimenti giudiziari e di contenzioso per cause passive portanti la richiesta di risarcimento danni.

4. Nella funzione (RSGI) Sistema Integrato Qualità, Sicurezza, Ambiente vengono trattati i seguenti dati personali:

a) dati anagrafici in senso stretto del lavoratore ed attestati rilasciati ai lavoratori relativi a corsi di formazione;
b) dati biometrici: si tratta di sole fotografie dei lavoratori, necessarie all'elaborazione dei tesserini di riconoscimento per l'accesso in sede ed in cantiere;
c) dati relativi alla salute, funzionali a verificare l'idoneità preassuntiva del lavoratore alle mansioni cui sarà assegnato e, a rapporto già instaurato, ad assolvere gli obblighi del datore di lavoro CAMPOLATTARO S.C.A.R.L. in tema di sicurezza derivanti dalla legge nonché relativi alle prestazioni di Pronto Soccorso in caso di infortunio.
d) Eventuali dati atti a rivelare le convinzioni religiose dei lavoratori, seppure fino ad ora mai verificatisi, laddove un lavoratore richieda permessi in orari definiti per esercitare il culto o di essere adibito a mansioni meno faticanti per periodi determinati per digiuni o altri costumi derivanti dall'esercizio del culto stesso.

5 La funzione di Presidente di CDA è una funzione apicale e di raccordo tra tutte le altre funzioni aziendali sottoposte. Il Presidente ha accesso a tutte le categorie di dati personali trattati dalla Società, e dunque, a titolo meramente esemplificativo, a dati relativi a:

a) personale dipendente;
b) fornitori ed affidatari;
c) compagnie assicurative ed Istituti Bancari;
d) professionisti e consulenti esterni.

6. Il Responsabile Lavori ha la funzione di seguire il regolare andamento del cantiere e del

personale impiegato nell'esecuzione delle opere e di conseguenza ha accesso ai seguenti dati personali:

a) dati anagrafici in senso stretto del lavoratore necessari alla sua identificazione personale per l'accesso ai cantieri e la rilevazione delle relative presenze;
b) dati relativi alla salute dei lavoratori funzionali a verificare l'idoneità sanitaria del lavoratore alle mansioni cui sarà assegnato e, a rapporto già instaurato, a permetterne il concreto svolgimento in cantiere
c) i dati biometrici: si tratta di sole fotografie dei lavoratori, necessarie all'elaborazione dei tesserini di riconoscimento per l'accesso in cantiere ed in sede;

7. Il Coordinatore per la sicurezza in fase di progettazione ed esecuzione in virtù del proprio ruolo gestisce, seppur in maniera limitata, il trattamento dei seguenti dati personali:
    a) dati anagrafici in senso stretto del lavoratore ed attestati rilasciati ai lavoratori relativi a corsi di formazione;
    b) dati biometrici: si tratta di sole fotografie dei lavoratori stampigliate sui tesserini di riconoscimento per l'accesso in cantiere.
8. I Sistemi informativi costituiscono il settore maggiormente colpito dal Regolamento in quanto tutti i dati gestiti dalle funzioni precedenti sono archiviati presso il server aziendale denominato "Campolattaro – F S01".

6 IL CONSENSO

Nel caso in cui il Trattamento dei Dati personali si fondi sul consenso al Trattamento espresso dall'Interessato, il Titolare deve essere in grado di dimostrare che l'Interessato abbia effettivamente fornito il suo consenso.

Il consenso reso dagli Interessati deve essere:

- ✓ Informato: ossia preceduto da adeguata informativa;

- ✓ Libero: ossia senza condizionamenti o vincoli;
- ✓ Specifico: ossia riferibile ad una singola finalità;
- ✓ Inequivocabile: ossia deve risultare certo che l'Interessato lo abbia prestato;
- ✓ Espresso: ossia non deve risultare dal silenzio o inattività dell'Interessato.

Nel caso in cui il consenso sia fornito nel quadro di una dichiarazione scritta riguardante anche altri temi, la richiesta di consenso dovrà essere presentata in maniera chiaramente distinguibile dagli altri temi, in una forma comprensibile e facilmente accessibile, con un linguaggio chiaro e semplice. È necessario altresì prevedere dei meccanismi che consentano all'Interessato di poter revocare in qualsiasi momento il consenso precedentemente prestato. La revoca del consenso non compromette la liceità del Trattamento sulla base del consenso prestato precedentemente. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al Trattamento di dati personali non necessario all'esecuzione di tale contratto. A tal riguardo i Destinatari sono tenuti ad assistere il Titolare in sede di raccolta del consenso da parte degli Interessati e di relativa conservazione dello stesso. Gli Autorizzati e i Data Manager, ove nominati, sono, inoltre, tenuti ad assistere il Titolare affinché lo stesso possa garantire il diritto di revoca del consenso eventualmente esercitato dagli Interessati nei confronti del Titolare.

Il consenso dovrebbe applicarsi a tutte le attività di Trattamento svolte per la stessa o le stesse finalità. Qualora il Trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la

richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è prestato.

Anche in tale ambito, andando oltre quanto strettamente indispensabile, CAMPOLATTARO S.C.A.R.L. ha predisposto modelli di consenso diversificati a seconda della categoria di interessati e delle specifiche finalità per la realizzazione delle quali il consenso viene prestato e ciò, al fine di renderlo quanto più consapevole ed informato possibile.

7 FORMAZIONE ED AGGIORNAMENTO DEL PERSONALE IN MATERIA DI PRIVACY

CAMPOLATTARO S.C.A.R.L., organizza la formazione e l'aggiornamento periodico di tutto il personale della Società in materia di Privacy. Per la formazione sulla Privacy sono previsti i seguenti contenuti minimi:

- formazione iniziale di almeno 2 ore al personale apicale e non apicale sul GDPR e sul MOGP adottato dall'ente;
- aggiornamento continuo di almeno 2 ore ogni triennio.

8 VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI E REGISTRO DELLE ATTIVITÀ

CAMPOLATTARO SCARL, al fine di tutelare i diritti e le libertà degli Interessati con riguardo al Trattamento dei Dati personali, attua adeguate misure tecniche e organizzative fin dal momento della progettazione del Trattamento stesso. Tutte le volte in cui un determinato tipo di Trattamento dei Dati personali possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei Dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi. La valutazione d'impatto è tesa a descrivere il Trattamento dei Dati personali, valutandone la necessità e la proporzionalità, nonché a contribuire alla gestione dei rischi per i diritti e le libertà

delle persone fisiche derivanti dal Trattamento stesso, valutando detti rischi e determinando le misure per affrontarla.

La valutazione d'impatto è tesa a descrivere il Trattamento dei Dati personali, valutandone la necessità e la proporzionalità, nonché a contribuire alla gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal Trattamento stesso, valutando detti rischi e determinando le misure per affrontarli.

Per conseguire sempre l'allineamento normativo e aumentare la capacità di controlli CAMPOLATTARO S.C.A.R.L. ha provveduto ad implementare il Registro dei Trattamenti finalizzato a mappare le diverse operazioni di trattamento dei Dati personali. Tale registro è un utile strumento per la completa ricognizione e valutazione dei Trattamenti effettuati e, pertanto, è finalizzato anche all'analisi del rischio e ad una corretta pianificazione dei Trattamenti. Il Titolare è responsabile alla corretta tenuta del Registro dei Trattamenti, nonché alla sua integrazione ed aggiornamento.

Ai sensi dell'Art. 30 RGPD il Registro dei Trattamenti contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del Titolare e, ove applicabile, del Contitolare del trattamento, del rappresentante del Titolare e del RPD;

b) le finalità del trattamento;

c) una descrizione delle categorie di Interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale, nonché la documentazione delle garanzie adeguate, ove applicabile;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative implementate.

A titolo esemplificativo: un rischio elevato potrebbe presentarsi qualora il trattamento comporti:

- l'uso di nuove tecnologie;
- la profilazione degli Interessati;
- il trattamento di dati sensibili o aventi carattere altamente personale;
- il monitoraggio sistematico degli Interessati (ivi inclusa la sorveglianza);
- il trattamento di dati relativi a Interessati vulnerabili.

Il Titolare è tenuto a conservare, sotto la sua responsabilità, tutta la documentazione inerente, conseguente ed accessoria alla valutazione d'impatto. Al fine di effettuare una valutazione d'impatto, il Titolare è tenuto ad effettuare:

- una descrizione sistematica dei Trattamenti previsti e delle finalità del Trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare.
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità perseguita;
- una valutazione dei rischi per i diritti e le libertà degli Interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei Dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli Interessati e delle altre persone in questione.

Nel caso in cui, all'esito della valutazione di impatto, il Titolare ritenga che il rischio non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e di costi di attuazione e

dovesse risultare dalla valutazione d'impatto che il trattamento (in mancanza delle garanzie, delle misure di sicurezza e dei meccanismi per attenuare il rischio) possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, dovrà ricorrere alla consultazione preventiva dell'Autorità ai sensi dell'art. 36 GDPR.

9. BANCHE DATI AZIENDALI E MODALITA' DI ARCHIVIAZIONE

La progressiva diffusione delle nuove tecnologie informatiche ed il libero accesso ad Internet tramite i Personal Computer, espone le informazioni trattate dalla Società e gli strumenti e supporti utilizzati per il loro trattamento a molteplici rischi e problemi legati alla sicurezza e alla fruibilità delle informazioni trattate.

La figura professionale che, in ambito informatico, mantiene, configura e gestisce un sistema di elaborazione dati o sue componenti, ivi inclusi sistemi software complessi (system administrator), ovvero una base dati (database administrator), ovvero reti e apparati di telecomunicazione di sicurezza (network administrator) è nominata persona autorizzata al trattamento dei dati personali con la qualifica specialistica di Amministratore di Sistema.

CAMPOLATTARO S.C.A.R.L. attribuisce le funzioni di Amministratore di Sistema dopo una attenta valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, affinché possa garantire il pieno rispetto delle vigenti disposizioni in materia, ivi compreso il profilo relativo alla sicurezza.

9.1. REGOLE PER I GLI UTENTI

Tutti gli Utenti ai quali è stato concesso di accedere alle risorse informatiche della Società, inclusi gli accessi ad Internet e l'utilizzo della posta elettronica aziendale, sono tenuti a rispettare le seguenti regole al fine di non incorrere in condotte non lecite.

Il comportamento dell'Utente lavoratore nell'utilizzo delle risorse informatiche messe a disposizione dovrà seguire i seguenti principi generali:

- l'Utente è responsabile dell'applicazione delle presenti regole ed è tenuto al rispetto delle norme comportamentali in esse contenute;
- l'Utente è responsabile dell'utilizzo delle risorse informatiche assegnategli;
- l'Utente è autorizzato ad accedere ai soli dati la cui conoscenza è necessaria all'espletamento delle mansioni attribuitegli;
- l'Utente, nell'utilizzo delle risorse informatiche, è tenuto a rispettare le seguenti regole:

a) non deve utilizzare gli strumenti di lavoro in violazione di leggi, né a rischio del la sicurezza del sistema informatico aziendale o, comunque, in modo tale da provocare danno all'immagine alla Società, ad altri lavoratori o a terzi;

b) deve adottare un comportamento a tutela della segretezza delle informazioni aziendali, con riferimento particolare al divieto di divulgare informazioni, anche tramite strumenti informatici;

c) deve applicare le misure di sicurezza adottate dalla Società al fine di evitare rischi di distruzione o perdita di dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta dei dati stessi;

d) non deve introdursi in sistemi informatici ai quali non è autorizzato ad accedere, in particolare se l'indebita intromissione o permanenza riguarda sistemi informatici o telematici protetti da misure di sicurezza;

e) non deve porre in essere azioni che possano danneggiare sistemi informatici della Società e altrui (ivi compresi programmi o dati altrui);

f) non deve impedire o alterare il funzionamento del sistema informatico, nonché intervenire senza diritto sui dati in esso contenuti;

g) non deve utilizzare o mettere a disposizione abusivamente codici di accesso (ad es. la password) o altri mezzi (ad es. badge) i quali permettono di accedere, in modo logico o fisico, a sistemi informatici protetti da misure di sicurezza e non deve altresì permettere o agevolare un indebito accesso ai predetti sistemi;

h) non deve utilizzare strumenti informatici se non preventivamente autorizzati dalla Società;

i) non deve scaricare da Internet o da qualsiasi altra rete telematica, riprodurre, duplicare, distribuire o memorizzare abusivamente opere di ingegno o parte di esso quali software o altro materiale in formato digitale (come ad esempio film o file musicali) tutelato dalle normative vigenti per la protezione del diritto d'autore;

j) tale divieto si intende esteso ed applicato nei termini sopra descritti a qualsiasi materiale digitale di provenienza illecita;

k) non deve utilizzare gli strumenti di comunicazione per offendere l'onore, il decoro o la reputazione di altri lavoratori o di terzi.

A seguito della cessazione del rapporto di lavoro, tutti i dati trattati devono rimanere a esclusiva disposizione della Società; inoltre l'Utente deve restituire tutte le strumentazioni informatiche affidategli.

9.2. CREDENZIALI DI ACCESSO (User- Id e Password)

L'Utente per accedere alle postazioni di lavoro, ai dispositivi mobili, ai sistemi applicativi e ai dati cui è stato autorizzato, deve avvalersi di "codici identificativi personali" (user-id), assegnati dall'Amministratore di Sistema, ai fini dell'identificazione univoca nell'ambito del sistema, e di "parole chiave" (password), con lo scopo di confermare la propria identità in fase di

autenticazione. Nell'ambito dell'accesso a ciascun servizio, l'utilizzo della user-id è soggetto ai seguenti vincoli:

- la user-id è assegnata individualmente e per uso strettamente personale;
- una volta assegnata, non può essere più riassegnata ad altri;
- non è permesso accedere con la stessa user-id, nello stesso momento, alla stessa applicazione da postazioni di lavoro diverse;
- è prevista una procedura volta a verificare periodicamente la validità delle autorizzazioni;
- in caso di non utilizzo per più di 90 giorni o al venire meno della necessità per cu i è stata assegnata. La user-id sarà disattivata manualmente, a seguito di precise istruzioni impartite dall'Amministratore di Sistema;

  qualora l'Utente ritenga che la segretezza della sua password sia stata compromessa deve darne comunicazione all'Amministratore di Sistema che provvederà al rilascio di una nuova password, la quale dovrà essere a sua volta modificata. A ciascuna user-id è associata una password, della cui segretezza e diligente custodia è responsabile l'utente: si ricorda che la password deve essere sostituita nel caso in cui se ne sospetti una perdita di segretezza.

9.3. NORME PER L'UTENTE

L'Utente, nella salvaguardia della sicurezza delle user-id assegnate, è tenuto a rispettare le seguenti regole:

- la user-id non deve essere divulgata, in quanto strettamente personale;
- qualora la user-id sia stata disattivata, l'Utente deve richiederne la riattivazione;
- in previsione della propria assenza definitiva o prolungata (dimissioni, quiescenza ecc.),

l'Utente deve supportare il proprio responsabile gerarchico per il passaggio di consegne prima che la user-id sia disabilitata.

L'Utente, per la salvaguardia della sicurezza delle proprie password, è tenuto a rispettare le seguenti regole:

- la password assegnata deve essere sostituita al primo accesso al sistema; -
- la password è personale e segreta per consentire l'accesso alle informazioni ed ai sistemi cui si è autorizzati: non è pertanto consentita la comunicazione della propria password ad altre persone, che potrebbero così agire in vece del reale proprietario; -
- non è consentito scrivere la password su carta o appunti o supporto liberamente accessibile;
- la password deve essere lunga almeno 8 caratteri, deve contenere almeno un carattere alfabetico ed almeno uno non alfabetico (caratteri speciali o numeri); per semplificarne la memorizzazione, possono essere usati numeri al posto delle lettere; -
- la password deve differire dalle ultime 3 password utilizzate, e non può contenere lo user-id;
- la password deve essere cambiata al più tardi ogni 3 mesi o comunque in linea con le vigenti normative (es. quelle in materia di tutela dei dati personali);
- la password non deve essere correlata a informazioni personali (es. nome, cognome o data di nascita) e deve essere differente da eventuali altre password utilizzate per fini personali (es. per l'accesso a siti Internet estranei all'attività lavorativa).

Nei casi di malfunzionamento del sistema di accesso o di smarrimento della propria password, si dovrà contattare l'Amministratore di Sistema per attuare le procedure atte alla salvaguardia della riservatezza della password.

9.4. TRATTAMENTO DEI DATI DEGLI UTENTI

CAMPOLATTARO S.C.A.R.L. esegue, al fine di garantire la continuità dell'attività lavorativa e la sicurezza del sistema ed in conformità con le normative in materia di tutela dei dati personali, il trattamento dei dati degli Utenti in riferimento all'utilizzo di Internet e della posta elettronica.

9.4.1. INTERNET

Le reti informatiche della Società sono protette da dispositivi che limitano l'accesso da parte di utenti non autorizzati (firewall). Le connessioni telematiche verso Internet sono presidiate da sistemi che tracciano la navigazione effettuata dagli Utenti aziendali in termini di pagine richieste (proxy server). Nei punti di accesso alla rete informatica aziendale operano dei filtri che limitano le connessioni telematiche solo a quelle espressamente autorizzate e bloccano le richieste indirizzate a siti Internet i cui contenuti confliggono con il decoro e l'immagine della Società (sistemi di controllo delle connessioni o web filtering).

L'accesso a Internet da parte degli Utenti può generare due tipologie di tracce (file di log):

a) file di log dei proxy server;
b) file di log dei dispositivi di controllo delle connessioni.

Tali tracce contengono un numero elevato di informazioni, di cui elenchiamo di seguito le più significative:

- la pagina Web richiesta;
- l'orario in cui è stata richiesta la pagina web;
- l'indirizzo di rete della postazione di lavoro ove è avvenuta la richiesta.

Si precisa che le informazioni tracciate non riguardano contenuti delle pagine web richieste, ma solo gli identificativi della pagina stessa.

9.4.2 POSTA ELETTRONICA

L'accesso al sistema di posta elettronica è gestito dai Sistemi Informativi delle società del Gruppo. Quando una email arriva dalla rete pubblica verso una postazione della rete interna della Società

attraversa i seguenti filtri:

- Antispam: nel caso in cui L'email sia riconosciuta come spam, tale sistema la registra nel proprio database. L'email resta nel data base per alcuni giorni per essere poi cancellata: ciò significa che un Utente ha pochi giorni di tempo per richiedere una email riconosciuta dal sistema come spam;
- Antivirus: se durante la scansione tale sistema individua un malware (virus, trojan, spyware, etc...) nella email in questione, dopo un periodo di quarantena, ne esegue la cancellazione in automatico;
- Repository della posta elettronica: L'email, dopo aver superato i controlli dei sistemi antispam e antivirus, viene memorizzata nel server di posta elettronica.

Il sistema antispam traccia un numero elevato di informazioni; quelle più rilevanti che riguardano l'Utente sono le seguenti:

- data e ora: fornisce l'indicazione temporale ovvero la data e ora in cui è avvenuto lo scambio del messaggio;
- indirizzo email del destinatario e del mittente: tramite questa informazione è possibile risa lire agli Utenti che si sono scambiati i messaggi email.

Il sistema antivirus raccoglie dati relativi alle possibili infezioni.

9.4.3. CONSERVAZIONE DEI DATI

I file log contenenti i dati personali relativi alla navigazione Internet ed all'utilizzo della posta elettronica sono conservati nei sistemi Proxy Server, Antispam, Antivirus, Mail server.

9.4.4 SICUREZZA DEI DATI

Tutti i file contenenti dati persona in riferimento ai log descritti in precedenza sono protetti da idonee misure di sicurezza, in particolare:

- in caso di anomalie, può avere accesso ai dati esclusivamente l'Amministratore di Sistema

per soli fini di verifica tecnica;

- i server di produzione ove risiedono i file di log sono collocati all'interno della rete protetta, il cui accesso è consentito unicamente all'Amministratore di Sistema.

10. AREE, LOCALI, STRUMENTI DI TRATTAMENTO

Il trattamento dei dati avviene, con le modalità di seguito riportate, sia presso la sede legale (Via Pietro Borsieri, 2 A- Roma), sia presso la sede operativa Contrada Collepiano n.18 Scala 5 – 82030 – TORRECUSO (BN), sia in tutti i cantieri attivi o che apriranno in futuro.

L'accesso agli uffici aziendali è consentito anche al pubblico attraverso n.2 entrate.

Gli uffici sono protetti da un sistema di allarme e da un servizio di telesorveglianza.

L'impianto di videosorveglianza installato presso la sede operativa del Consorzio è composto da n.6 telecamere.

L'impianto è in funzione 24 ore su 24, essendo configurato per la registrazione continuativa.

La rilevazione e registrazione delle immagini avviene senza il consenso dell'interessato in quanto l'interesse perseguito è quello della protezione delle persone e del patrimonio aziendale da possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, prevenzione di incendi e sicurezza del lavoro.

Nei cantieri l'acceso è consentito solamente agli addetti autorizzati. I cantieri sono presidiati da servizio di guardiania. da un servizio di telesorveglianza. L'ingresso dei dipendenti, dopo il passaggio dal posto di guardiania, viene registrato dai badge situati all'interno dell'edificio.

Con riferimento agli strumenti utilizzati e alle tipologie dei dati trattati si precisa che:

1. i dati comuni vengono trattati sistematicamente con supporti cartacei e con elaboratori;

2.i dati sensibili trattati sistematicamente con supporti cartacei e con elaboratori sono esclusivamente relativi ai dipendenti per la gestione delle attività contabili, fiscali, amministrative, connesse al rapporto di lavoro e giudiziari, afferenti all'ufficio legale, per gli adempimenti ex L.

55/90;

3. gli elaboratori in rete presenti sono collegati in rete con altri e dispongono esclusivamente del collegamento ad INTERNET filtrato da sistemi anti-intrusione (firewall).

Di seguito una tabella riassuntiva della struttura competente al trattamento dati e la relativa descrizione del trattamento:

Struttura competente	Descrizione sintetica
Acquisti - Contrattualistica e Protocollo di Legalità	Raccolta, organizzazione, conservazione, consultazione, modificazione, utilizzo, comunicazione, diffusione, cancellazione dei dati relativi ai rapporti contrattuali con fornitori, appaltatori, affidatari ed Istituti di credito.
Amministrazione e Finanza	Raccolta, organizzazione, conservazione, consultazione, modificazione, utilizzo, comunicazione, cancellazione dei dati relativi a offerte/contratti di finanziamento, istituti di credito finanziatori, documenti di garanzia, versamenti. Elaborazione F24, dichiarazioni fiscali, certificazione ritenute, home banking, fornitori e appaltatori.

Archivio Generale	Raccolta, organizzazione, scannerizzazione, archiviazione, distribuzione di tutti i documenti amministrativi e della corrispondenza in entrata e in uscita.
Comitato Tecnico	Tutti i dati inerenti la gestione tecnico-economico finanziaria dei lavori.
Comunicazione	Raccolta, organizzazione, elaborazione, conservazione, consultazione, modificazione, utilizzo, comunicazione, diffusione, di dati relativi alla gestione delle comunicazioni da/vs enti/altri soggetti.
Consulente assicurativo	Gestione dati relativi a Compagnie di assicurazione e cauzione, Istituti di credito.
Coordinatore per la sicurezza in fase di progettazione ed esecuzione (CSP/CSE)	Raccolta, organizzazione, conservazione, consultazione dei dati relativi al cantiere e al personale impiegato nell'esecuzione delle opere.

Direzione lavori	Gestione dei dati relativi agli aspetti legali e procedure antimafia, dati inerenti la contabilità lavori, gli espropri, le prove e collaudi, monitoraggio lavori, tutti i dati relativi alle diverse fasi contrattuali oltre a quelli strettamente connessi all'esecuzione delle opere.
Internal Auditing	Gestione dei dati relativi al personale dipendente, fornitori, affidatari, Ente Appaltante, Istituti di Credito, Compagnie di assicurazione e cauzione, OO.SS., Consulenti esterni.
Organismo di vigilanza	Gestione dei dati relativi al personale dipendente, fornitori, affidatari, Ente Appaltante, Istituti di Credito, Compagnie di assicurazione e cauzione, OO.SS., consulenti esterni.
Project Manager Construction manager	Raccolta, organizzazione, conservazione, consultazione, modificazione, utilizzo, comunicazione, diffusione, cancellazione dei dati relativi alla programmazione economico-finanziaria ed al controllo della commessa, di quelli relativi alla progettazione, pianificazione e gestione delle tratte.
Responsabile Lavori	Raccolta, organizzazione, conservazione, consultazione dei dati relativi al cantiere e al personale impiegato nell'esecuzione delle opere.

Risorse Umane	Raccolta, organizzazione, conservazione, consultazione, modificazione, utilizzo, comunicazione, cancellazione dei dati anagrafici, di domiciliazione bancaria, di dati reddituali, contributivi ed assistenziali del personale: - Registrazione presenze - Trasmissione dati- Gestione buste paga - Selezione e sviluppo personale.
Segreteria	Raccolta, organizzazione, conservazione, consultazione, modificazione, utilizzo, comunicazione, cancellazione dei dati di competenza dell'AD.
Servizi generali	Distribuzione di tutti i documenti amministrativi e della corrispondenza in entrata e in uscita.
Servizio Portineria	Archiviazione dei dati di accesso del personale, visitatori e collaboratori.
(RSGI) Sistema Integrato Qualità – Sicurezza- Ambiente	Tutti i dati relativi ai processi aziendali ed alle procedure del Sistema di gestione per la Qualità, inclusi quelli inerenti la formazione ed addestramento del personale.

Ufficio Legale	Raccolta, organizzazione, cancellazione dei dati relativi a contenziosi giudiziari ed arbitrali, dei dati contrattuali, dei dati relativi agli affidatari, ai rapporti con gli appaltatori, agli adempimenti ex L. 55/90 (antimafia), degli adempimenti amministrativi/legali relativi al protocollo di legalità.

11. MISURE DI SICUREZZA ADOTTATE

Alla luce dei fattori di rischio e delle aree individuate nel presente Modello vengono descritte le misure atte a garantire:

- la protezione delle aree e dei locali ove si svolge il trattamento dei dati personali;
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali
- la sicurezza logica, nell'ambito degli strumenti elettronici.

Per quanto concerne il rischio che i dati vengano danneggiati o perduti a seguito di eventi distruttivi, i locali ove si svolge il trattamento dei dati sono protetti da:

- dispositivi antincendio previsti dalla normativa vigente;
- gruppo di continuità dell'alimentazione elettrica;
- impianto di condizionamento.

Per il trattamento effettuato con strumenti elettronici sono esistenti ed operative le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica al fine di accertare l'identità delle persone che hanno accesso agli strumenti elettronici (profilo di accesso per

la rete e per i software applicativi e gestionali);

- le policy dell'azienda garantiscono la sicurezza di tutti i dati circolanti, attraverso il controllo delle autorizzazioni e la definizione delle tipologie di dati ai quali gli incaricati possono accedere e utilizzare secondo le mansioni lavorative;
- protezione di strumenti e dati da malfunzionamenti ed attacchi informatici attraverso firewall e antivirus centralizzati;
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili, contenenti dati personali.

L'articolo 33 del GDPR prevede quanto segue:

- In caso di violazione dei dati personali, il Titolare del Trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo
- Il responsabile del Trattamento informa il Titolare del Trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione;
- La notifica al Garante deve almeno:
  a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
  b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
  c) descrivere le probabili conseguenze della violazione dei dati personali;
  d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del

Trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

- Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo;
- Il Titolare del Trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

L'articolo 34, in merito alla comunicazione di una violazione dei dati personali all'interessato, prevede invece quanto segue:

- Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento comunica la violazione all'interessato senza ingiustificato ritardo;
- la comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33;

Non è richiesta la comunicazione all'interessato di cui se è soddisfatta una delle seguenti condizioni:

a) il Titolare del Trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il Titolare del Trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli

interessati sono informati con analoga efficacia;

d) 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 sopra individuate sia soddisfatta.

12. INOSSERVANZA DELLA POLICY PRIVACY

Il presente Modello Organizzativo Privacy si applica all'azienda nella sua interezza a tutti gli organi e alle strutture di qualsiasi livello organizzativo o funzionale.

La sua attuazione è obbligatoria per tutto il personale e deve essere inserita come parte integrante nella regolamentazione di qualsiasi accorsi con tutti i soggetti esterni coinvolti con il trattamento di informazioni che rientrano nel campo del Sistema di Gestione della Privacy.

CAMPOLATTARO SCARL consente la comunicazione e la diffusione delle informazioni di tipo procedurale e organizzativo verso l'esterno esclusivamente per il corretto svolgimento delle attività aziendali che avvengono nel rispetto delle regole e delle norme vigenti.

Eventuali violazioni della presente Policy, possono avere gravi ripercussioni sulla Società e comportare, nei confronti del dipendente inadempiente, l'applicazione di provvedimenti disciplinari, in conformità alle disposizioni di legge e del CCNL applicabile e nei confronti degli altri Destinatari anche la cessazione del rapporto contrattuale. I comportamenti che costituiscono violazione della presente Policy possono determinare, nel contempo, la violazione di disposizioni di legge tali da implicare per l'utilizzatore inadempiente conseguenze di natura civile e penale. Anche la Società può essere perseguita e sanzionata in conseguenza della condotta dei Destinatari. Agli stessi potrà dunque venire richiesto di

risarcire i danni derivati dalle violazioni della presente Procedura.

Il presente Modello Organizzativo Privacy è soggetto a verifica ed eventuale aggiornamento annuale.