MODELLO ORGANIZZATIVO PRIVACY

AI SENSI DEL

REGOLAMENTO 679/2016 (GDPR)

Approvato il 6 novembre 2023

MODELLO ORGANIZZATIVO PRIVACY

Sommario

ALLEGATI

1. MATRICE DEI RISCHI
2. ORGANIGRAMMA PRIVACY
3. PROCEDURA DI DISASTER RECOVERY E BUSINESS CONTINUITY
4. FAC-SIMILE INFORMATIVA E CONSENSO
5. FAC-SIMILE NOMINA A RESPONSABILE DEL TRATTAMENTO
6. FAC-SIMILE NOMINA A RESPONSABILE INTERNO DEL TRATTAMENTO
7. PROCEDURA DATA BREACH, CANCELLAZIONE E PORTABILITÀ DEI DATI

1. PREMESSA

Il presente **Modello Organizzativo Privacy** raccoglie le ***misure tecniche ed organizzative*** che METRO C S.c.p.A. 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 la Società effettua direttamente o tramite soggetti terzi debitamente legittimati.

Il Regolamento del 27 aprile 2016, cosiddetto **"*General Data Protection Regulation*"** (di seguito brevemente "*GDPR*" o "Regolamento"), pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016, è divenuto definitivamente operativo ed applicabile in via diretta in tutti i Paesi membri dell'Unione Europea a partire dal 25 maggio 2018 e persegue il fine di rafforzare la protezione dei dati personali delle persone fisiche, sia all'interno che all'esterno dei confini europei, dunque a prescindere dal principio di territorialità, armonizzando le regole *privacy* di tutti gli Stati membri.
Insieme alla più settoriale Direttiva UE 2016/680 dello stesso giorno, inerente al trattamento dei dati personali nelle attività di polizia e giudiziarie, il Regolamento in oggetto costituisce il c.d. "*pacchetto protezione dati personali".*

Nell'ordinamento italiano è, inoltre, successivamente intervenuto il Decreto Legislativo 10 agosto 2018, n. 101 recante *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679"*, pubblicato in Gazzetta Ufficiale il 4 settembre 2018 ed entrato in vigore il 19 settembre 2018, allo scopo di coordinare la normativa comunitaria con il previgente Codice Privacy introdotto con il D. Lgs. n. 196/2003 e di dirimere le incertezze interpretative derivate dalla sovrapposizione delle norme, comunitarie da un lato e nazionali dall'altro, che costituiscono l'attuale quadro normativo.

L'adozione delle ***misure tecniche ed organizzative adeguate*** è imposta dagli artt. 24 e seguenti del GDPR, ai sensi dei quali le **politiche interne** e le **misure da attuare** per soddisfare i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita, 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 interessate.
Al fine di rispettare tale requisito, pertanto, l'elaborazione della **prima versione** del presente modello, approvato dalla Società il 23 maggio 2018, ha richiesto la preventiva esecuzione di una attenta e critica attività di *auditing*, che ha consentito l'esame della singola realtà aziendale e la valutazione dei rischi cui sono potenzialmente esposti gli interessati, laddove per *"rischio"* si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità per i diritti e le libertà (Linee guida del Gruppo di lavoro Articolo 29 WP248 rev.1).

Il Modello, giunto ora alla **seconda edizione**, viene sottoposto a revisione integrale, al fine di aggiornarne i contenuti sia alla normativa *medio tempore* intervenuta, rappresentata dal citato D. Lgs. n. 101/2018, successivo alla prima edizione, che alla modifica organizzativa che la Società ha in corso di realizzazione rappresentata dalla rilevante attività di aggiornamento e riorganizzazione dei sistemi informativi, precedentemente mutuati da uno dei propri soci.
La seconda edizione del presente Modello Organizzativo Privacy, inoltre, intende tener conto, per finalità di semplificazione, delle pronunce nel frattempo emesse, a livello comunitario, dal Comitato europeo per la protezione dei dati (EDPB) e, a livello nazionale, dall'Autorità Garante per la protezione dei dati personali all'indomani dell'intervento legislativo di coordinamento.

La redazione della prima versione, infatti, inserendosi in un contesto normativo a suo tempo ancora incerto ed *in fieri*, si era ispirata al principio di massima prevenzione, in ossequio al principio di responsabilizzazione del titolare del trattamento, prevedendo processi e adempimenti volti a garantire la liceità dei trattamenti e la protezione dei dati ancor più articolati di quanto strettamente necessario.

All'indomani dell'intervento legislativo di coordinamento attuato con il D. Lgs. n. 101/2018 e dei provvedimenti delle Autorità, europea ed italiana, si è determinata una migliore definizione del perimetro normativo di riferimento che consente ora a Metro C, da un lato, di semplificare i propri processi e, dall'altro, aumentare il livello di protezione dei dati trattati mediante strumenti informatici e telematici: fattori essenziali in proposito risultano essere, in primo luogo, l'Autorizzazione Generale n. 1/2016 che, sottoposta a verifica di compatibilità con le disposizioni del Regolamento, è stata confermata dall'Autorità Garante della Protezione dei dati personali con provvedimento n. 146 del 5 giugno 2019, che consente al datore di lavoro di trattare legittimamente, in ambito lavorativo, i dati personali dei propri collaboratori e, in secondo luogo, la rilevante attività di aggiornamento e riorganizzazione dei sistemi informativi della Società secondo i migliori e più avanzati standard di sicurezza.

Nell'ambito di tale mutato contesto, METRO C ha inoltre inteso ora riesaminare altresì la valutazione dei rischi che era stata elaborata in occasione della prima edizione, funzionale all'individuazione delle misure tecniche ed organizzative necessarie a mitigarli, e ciò allo scopo di evidenziare, con immediata evidenza, l'impatto che l'implementazione organizzativa determina in riferimento alla protezione ed alla sicurezza dei dati giudiziari trattati da Metro C in adempimento degli obblighi ed oneri assunti in virtù dei Protocolli Antimafia di cui appresso: prendendo spunto da tale necessità, in ottica di continuo ed ulteriore miglioramento in ordine alla propria *accountability*, la matrice dei rischi a suo tempo elaborata da METRO C è stata arricchita di un'apposita ed ulteriore sezione, dedicata alla valutazione dei rischi per i diritti e le libertà delle persone interessate dal trattamento di tali dati, caratterizzati da un grado di delicatezza e riservatezza del tutto peculiari. L'obiettivo di tale ulteriore analisi, condotta su base volontaria e realizzata come buona prassi al di là dei requisiti di legge, ha consentito di guardare allo stesso oggetto - ossia al concetto *"rischio"* - sotto due distinti angoli visuali: uno, interno, di cui già accennato, dal senso organizzativo e prodromico alla realizzazione delle azioni interne di mitigazione intraprese da METRO C; l'altro, esterno, che guarda alla tutela preventiva dei diritti e delle libertà degli interessati al fine di ricavare indicazioni importanti ed utili a prevenire incidenti futuri, garantendo la protezione dei dati fin dalla fase di progettazione (*data protection by design*) di qualsiasi trattamento da essa effettuato e da sottoporre a revisione continua.

1.1 DEFINIZIONI

Ai fini del GDPR ed in relazione ai concetti specificamente coinvolti dalle attività di trattamento effettuate, direttamente ed indirettamente da METRO C S.c.p.A., ai sensi dell'art. 4 del GDPR si intendono per:

1) ***«dato personale»***: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

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

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

4) ***«profilazione»***: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) ***«pseudonimizzazione»***: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) ***«archivio»***: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) ***«titolare del trattamento»***: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) ***«responsabile del trattamento»***: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) ***«destinatario»***: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

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

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

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

13) ***«dati genetici»***: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano, in particolare, dall'analisi di un campione biologico della persona fisica in questione;

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

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

16) ***«stabilimento principale»***:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

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

18) ***«impresa»***: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) ***«gruppo imprenditoriale»***: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) ***«norme vincolanti d'impresa»***: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) ***«autorità di controllo»***: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento;

22) ***«autorità di controllo interessata»***: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

c) un reclamo è stato proposto a tale autorità di controllo.

1.2. GENERAL DATA PROTECTION REGULATION (GDPR)

Il GDPR è costituito da ***tre principi ispiratori,*** che permeano e sostengono l'***intero impianto normativo*** ed il cui rispetto è protetto da un sistema sanzionatorio, delineato dagli artt. 83 e ss. del Regolamento, 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, ove il fatto commesso costituisca reato, previste dal D. Lgs. n. 196/2003, come modificato dal D. Lgs. n. 101/2018.

Tali principi essenziali sono quelli di:

1) ***accountability***, ossia il principio di responsabilizzazione: il Regolamento non effettua una tipizzazione puntuale ***delle misure tecniche e organizzative,*** esprimendosi unicamente in termini di loro ***adeguatezza*** al rischio *"tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche"* (art. 32 GDPR). Si tratta di una innovazione profonda in quanto viene attribuito ai Titolari il compito di decidere autonomamente le modalità, le garanzie ed i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative ed alla luce di alcuni criteri specifici indicati nel Regolamento. Ciò impone un approccio integrato, che interessi tutte le aree aziendali, concreto e *risk-based* e che dia luogo a comportamenti proattivi;

2) ***privacy by design***, che impone l'adozione di misure di protezione fin dalla fase di progettazione del trattamento;

3) ***privacy by default***, che prescrive un utilizzo che si limiti, per impostazione predefinita, ai soli dati necessari a rispondere alle finalità specifiche della gestione dei dati.

Tali principi si traducono nell'assunto in base al quale ogni trattamento di dati personali debba avvenire, potendolo dimostrare anche *ex post*, nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/, ossia:

a. liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;

b. limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;

c. minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;

d. esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;

e. limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;

f. integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

In particolare, il trattamento è ***lecito*** allorché trovi fondamento in una idonea ***base giuridica*** (art. 6 Reg.) che, fermo restando in ogni caso l'obbligo di informativa a carico del Titolare del trattamento, può consistere in:

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*";

2) ***adempimento di obblighi contrattuali o precontrattuali***, 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 definita per legge, spettando al titolare del trattamento individuarla nello specifico;

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 ed 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.

Per garantire la correttezza e la trasparenza dei trattamenti è dunque necessario che gli interessati siano informati, prima ancora dell'inizio del trattamento stesso, in merito all'**identificazione** dei dati personali che saranno oggetto di successivo trattamento, alle relative **finalità** perseguite, alle **modalità** del trattamento, all'**identità del titolare** del trattamento, al successivo **flusso** cui i dati saranno sottoposti, alle modalità di loro **conservazione** fino alla **cancellazione**, alle modalità di esercizio dei loro **diritti**: tali informazioni devono essere esplicitate nell'informativa che il titolare deve sempre rendere loro, peraltro in maniera semplice, chiara e facilmente comprensibile, in modo da garantire loro il controllo dei propri dati per tutto il loro ciclo di vita.

L'interessato deve, perciò, 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 siano eventualmente detenuti dal titolare, *"perché"* e *"come li abbia avuti"*.

A livello operativo, tali principi si concretizzano nelle seguenti azioni:

a) adempimento dell'***obbligo preventivo di informativa*** (artt. 13 e 14 Reg.), da rendere sempre ed obbligatoriamente, tutte le volte in cui debba essere iniziato il trattamento, non necessariamente per iscritto ma con forme documentabili *ex post*;

b) istituzione del ***Registro delle attività di trattamento*** (art.30 Reg. 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;

c) designazione dei ***Responsabili del trattamento*** (art. 28 Reg.), indispensabile a legittimare tutti i soggetti terzi che effettuano trattamenti di dati personali per conto del titolare, che devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che i trattamenti soddisfino i requisiti del Regolamento e garantiscano la tutela dei diritti dell'interessato;

d) ***formazione*** ed ***autorizzazione*** dei soggetti incaricati, interni alla struttura del titolare e/o al responsabile che, agendo sotto la loro autorità, hanno accesso ai dati (art. 29 Reg.). Fondamentale rilievo assume, in proposito, lo svolgimento di specifiche attività di formazione ed informazione a beneficio di tutti i soggetti autorizzati;

e) designazione del ***Responsabile della protezione dei dati personali*** (*Data Protection Officer*, artt. 37-39 Reg.) intesa come figura fondamentale che deve raccogliere in sé competenze normative, tecniche, comunicative e di conoscenza profonda della struttura e dell'organizzazione aziendale;

f) formalizzazione della disciplina del ***processo di data breach,*** (artt. 33 e 34 Reg.) ossia della 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, la cui predisposizione consente una gestione tempestiva e ponderata dell'evento e delle sue conseguenze, compresa la notifica all'Autorità Garante.

2. OBIETTIVO E STRUTTURA DEL MODELLO

L'obiettivo del presente **Modello Organizzativo Privacy** è di garantire e dimostrare che il trattamento dei dati personali da parte di METRO C S.c.p.A. avviene in modo lecito, corretto e trasparente secondo la definizione sopra datane, da raggiungere attraverso la realizzazione di una gestione interna ben strutturata che promuova la **cultura della privacy** e della **sicurezza dei dati personali**, consolidando i principi comportamentali idonei a garantire la trasparenza, la sicurezza e la correttezza dei trattamenti, aumentando la propria affidabilità verso i propri azionisti, clienti, *partners*, consulenti e dipendenti.

Con l'ulteriore conseguenza di **evitare la possibile erogazione delle sanzioni amministrative** pecuniarie di cui all'art. 83 GDPR **nonché di quelle penali di cui al vigente D. Lgs. n. 196/2003** potendo, con la sua adozione, dimostrare l'attuazione concreta, efficiente ed efficace delle misure tecniche ed organizzative adeguate alla

protezione dei dati personali da essa trattati, direttamente o tramite soggetti terzi che li effettuano per suo conto.

Il presente Modello Organizzativo si compone di ***nove sezioni*** dirette a fornire una panoramica sul sistema complessivo delle ***misure tecniche e organizzative che, sulla base delle concrete esigenze sistematiche ed operative di METRO C, 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 Modello è organizzato come segue:

- sez. 1, contenente alcuni **cenni generali** sui principi ispiratori del GDPR;
- sez. 2, illustrativa della **struttura** del presente Modello;
- sez. 3, dedicata alla **policy aziendale**, ossia all'esposizione dei principi generali di condotta adottati da METRO C S.c.p.A. nel trattamento dei dati personali in relazione alla loro tipologia;
- sez. 4, illustrativa delle **figure** privacy coinvolte;
- sez. 5, rivolta all'analisi delle **funzioni e dei processi** interessati secondo le risultanze dell'**organigramma privacy**;
- sez. 6, dedicata all'illustrazione delle risultanze del ***risk assessment;***
- sez. 7, contenente l'elencazione delle **banche dati aziendali** e l'illustrazione delle **modalità di archiviazione** dei dati;
- sez. 8, di approfondimento delle **modalità** e degli **strumenti di trattamento** dei dati, anche sotto il profilo **spaziale**;
- sez. 9, concernente le **misure di sicurezza** a presidio dei rischi come sopra rilevati;

Vi si aggiungono ***sette allegati*** contenenti indicazioni più strettamente operative, avendo la funzione di enunciare le specifiche regole tecniche e di condotta che tutti i soggetti operanti in METRO C S.c.p.A., ad ogni livello, sono tenuti ad osservare al fine di evitare la commissione di violazioni del Regolamento e la conseguente sottoposizione al regime sanzionatorio.

In particolare,

1. Matrice dei Rischi
2. Organigramma Privacy
3. *nuova* Procedura di Disaster Recovery e Business Continuity *in bozza*, che alla data di approvazione del presente Modello è in corso di valutazione tecnica e di testing, essendo operativa la precedente versione già allegata alla prima edizione del presente Modello
4. Fac-simile Informative e Consensi
5. Fac-simile Nomina a Responsabile del Trattamento
6. Fac-simile Nomina a Responsabile Interno del Trattamento
7. Procedura di Data Breach, Cancellazione e Portabilità dei Dati

Allegati e fac-simili sono destinati a costituire per gli operatori di ogni livello gerarchico una utile guida pratica da adattare, poi, alle singole esigenze concrete ed alle necessità che, tempo per tempo, sopravverranno, in armonia con ***i principi di effettività e concretezza*** che animano l'intero impianto normativo del GDPR, che ne impone il costante monitoraggio ed aggiornamento.

3. POLICY AZIENDALE

METRO C S.c.p.A. è una società di progetto costituita per la realizzazione della nuova linea C della Metropolitana di Roma per conto della Committente Roma Metropolitane. Per il perseguimento del proprio scopo, pertanto, METRO C S.c.p.A. svolge tutte le attività a ciò necessarie tra le quali – per quanto qui interessa:

- l'acquisizione e la gestione delle risorse umane;
- l'approvvigionamento degli strumenti, dei materiali, dei servizi e dei lavori;
- l'appalto di parti dell'opera ad imprese specializzate ed i relativi sub-appalti;
- la realizzazione concreta dell'opera.

"QUALI" DATI E "PERCHE'"

Nello svolgimento di tali attività, METRO C S.c.p.A. gestisce differenti tipologie di dati personali, ovvero:

a. ***Dati comuni***
ossia dati anagrafici in senso stretto (nome, cognome, luogo e data di nascita, codice fiscale, domicilio o residenza) 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.
Il trattamento di tale tipologia di dati si rende necessaria per l'esecuzione dei contratti di cui Metro C, da un lato, e gli interessati, dall'altro, sono parte (ad es. contratti di lavoro, di appalto) e per l'adempimento degli obblighi di legge di cui è parte la stessa società Metro C (ad es. rilevazione delle presenze presso la sede ed in cantiere per finalità di sicurezza).

b. ***Dati bancari***
che si concretizzano nelle coordinate bancarie dei lavoratori e dei fornitori, indispensabili al pagamento di compensi, stipendi, salari, emolumenti di qualsiasi natura da loro maturati e dovuti a titolo di corrispettivo per beni o servizi resi a METRO C. Si tratta certamente di dati personali, in quanto idonei ad identificare inequivocabilmente la persona dell'interessato ma non possono considerarsi *"categorie particolari di dati personali*" (comunemente definiti sotto la previgente normativa come *dati sensibili*) in quanto la semplice coordinata bancaria di cui METRO C dispone non è in grado di rivelare informazioni ulteriori rispetto alle semplici spettanze oggetto di pagamento.

c. ***Categorie particolari di dati personali***
riferibili ai lavoratori inquadrati ad ogni livello aziendale. Si tratta dei dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona stessa. La base giuridica del trattamento, finalizzato alla gestione dei rapporti di lavoro, è costituita dalla necessità di assolvere gli obblighi ed esercitare i diritti specifici di Metro C, quale titolare del trattamento, o del lavoratore interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale (art. 9, comma 2, lett. b).

In proposito, come accennato, particolare importanza è ricoperta dal provvedimento del Garante che individua le prescrizioni contenute, tra le altre, nell'***Autorizzazione generale n. 1/2016***, che risultano compatibili con il GDPR e con il D.lgs. n. 101/2018 di adeguamento del Codice e che Metro C, nel trattamento di tali dati, osserva.

Tale provvedimento, emanato il 13 dicembre 2018 – quindi, successivamente alla prima edizione del presente Modello - legittima il trattamento di categorie particolari di dati personali nel contesto lavorativo per finalità d'instaurazione, gestione ed estinzione del rapporto di lavoro stesso, riferibili a **candidati** (anche in caso di curricula spontaneamente trasmessi dagli interessati), **lavoratori subordinati** (anche se parti di un contratto di apprendistato, di formazione, a termine, di lavoro intermittente, di lavoro occasionale, ovvero prestatori di lavoro nell'ambito di un contratto di somministrazione di lavoro, o in rapporto di tirocinio, ovvero ad associati anche in compartecipazione), **consulenti e liberi professionisti, agenti, rappresentanti e mandatari**; soggetti che svolgono collaborazioni organizzate dal committente, o altri **lavoratori autonomi** in rapporto di collaborazione, persone fisiche che ricoprono **cariche sociali** o altri incarichi, **terzi danneggiati** nell'esercizio dell'attività lavorativa o professionale dai soggetti sopra indicati, terzi (**familiari o conviventi** dei soggetti sopra indicati per il rilascio di agevolazioni e permessi).

In estrema sintesi, è legittimo il trattamento delle categorie particolari di dati personali riferibili alle persone sopra indicate da parte di Metro C, quale datore di lavoro, quando vengono rispettate le condizioni appresso descritte, inerenti alle finalità del trattamento ed alle prescrizioni specifiche:

- *Finalità del trattamento*

  Il trattamento delle categorie particolari di dati personali è effettuato solo se necessario:

  - per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa europea, nazionale o da contratti collettivi anche aziendali, ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro, del riconoscimento di agevolazioni ovvero dell'erogazione di contributi, dell'applicazione della normativa in materia di previdenza ed assistenza anche integrativa, o in materia di igiene e sicurezza del lavoro, nonché in materia fiscale e sindacale;
  - ai fini della tenuta della contabilità o della corresponsione di stipendi, assegni, premi, altri emolumenti, liberalità o benefici accessori;
  - per perseguire finalità di salvaguardia della vita o dell'incolumità fisica del lavoratore o di un terzo;
  - per far valere o difendere un diritto, anche da parte di un terzo, in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione, nei casi previsti dalle leggi, dalla normativa dell'Unione europea, dai regolamenti o dai contratti collettivi, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento; il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose;
  - per adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di salute e sicurezza del lavoro e di malattie professionali o per i danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale;
  - per garantire le pari opportunità nel lavoro;
  - per perseguire scopi determinati e legittimi individuati dagli statuti di associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro o dai contratti collettivi, in materia di assistenza sindacale ai datori di lavoro.

- *Prescrizioni specifiche relative alle categorie di dati*

Nella fase preliminare alle assunzioni

- i dati idonei a rivelare lo stato di salute e l'origine razziale ed etnica dei candidati all'instaurazione di un rapporto di lavoro o di collaborazione possono essere trattati solo se la loro raccolta sia giustificata da scopi determinati e legittimi e sia necessaria per instaurare tale rapporto;
- siano raccolte le sole informazioni strettamente pertinenti e limitate a quanto necessario a tali finalità, anche tenuto conto delle particolari mansioni e/o delle specificità dei profili professionali richiesti;
- qualora nei curricula inviati dai candidati siano presenti dati non pertinenti rispetto alla finalità perseguita, il datore di lavoro che effettua la selezione deve astenersi dall'utilizzare tali informazioni;
- i dati genetici non possono essere trattati al fine di stabilire l'idoneità professionale di un candidato all'impiego, neppure con il consenso dell'interessato.

Nel corso del rapporto di lavoro

- I dati che rivelano le convinzioni religiose o filosofiche ovvero l'adesione ad associazioni od organizzazioni a carattere religioso o filosofico possono essere trattati esclusivamente in caso di fruizione di permessi in occasione di festività religiose o per le modalità di erogazione dei servizi di mensa o, nei casi previsti dalla legge, per l'esercizio dell'obiezione di coscienza;
- I dati che rivelano le opinioni politiche o l'appartenenza sindacale, o l'esercizio di funzioni pubbliche e incarichi politici, di attività o di incarichi sindacali esclusivamente ai fini della fruizione di permessi o di periodi di aspettativa riconosciuti dalla legge o, eventualmente, dai contratti collettivi anche aziendali nonché per consentire l'esercizio dei diritti sindacali compreso il trattamento dei dati inerenti alle trattenute per il versamento delle quote di iscrizione ad associazioni od organizzazioni sindacali;
- in caso di partecipazione di dipendenti ad operazioni elettorali in qualità di rappresentanti di lista, in applicazione del principio di necessità, il datore di lavoro non deve trattare nell'ambito della documentazione da presentare al fine del riconoscimento di benefici di legge, dati che rivelino le opinioni politiche (ad esempio, non deve essere richiesto il documento che designa il rappresentante di lista essendo allo scopo sufficiente la certificazione del presidente di seggio);
- il datore di lavoro non può trattare dati genetici al fine di stabilire l'idoneità professionale di un dipendente, neppure con il consenso dell'interessato.

Modalità di trattamento

- i dati devono essere raccolti, di regola, presso l'interessato;
- in tutte le comunicazioni all'interessato che contengono categorie particolari di dati devono essere utilizzate forme di comunicazione anche elettroniche individualizzate nei confronti di quest'ultimo o di un suo delegato, anche per il tramite di personale autorizzato. Nel caso in cui si proceda alla trasmissione del documento cartaceo, questo dovrà essere trasmesso, di regola, in plico chiuso, salva la necessità di acquisire, anche mediante la sottoscrizione per ricevuta, la prova della ricezione dell'atto;
- i documenti che contengono dati categorie particolari di dati, ove debbano essere trasmesse ad altri uffici o funzioni in ragione delle rispettive competenze, devono contenere esclusivamente le informazioni necessarie allo svolgimento della funzione senza allegare, ove non strettamente indispensabile, documentazione integrale o riportare stralci all'interno del testo;
- quando per ragioni di organizzazione del lavoro, e nell'ambito della predisposizione di turni di servizio, si proceda a mettere a disposizione a soggetti diversi dall'interessato (altri colleghi) dati relativi a presenze ed assenze dal servizio, il datore di lavoro non deve esplicitare, nemmeno

attraverso acronimi o sigle, le causali dell'assenza dalle quali sia possibile evincere la conoscibilità di particolari categorie di dati personali (es. permessi sindacali o dati sanitari).

L'emanazione di tale provvedimento ha consentito di semplificare notevolmente gli adempimenti privacy a carico di METRO C – datore di lavoro, ora non più chiamato a raccogliere il consenso dei propri lavoratori che, anteriormente all'intervento del Garante, veniva richiesto per il trattamento delle categorie particolari di dati personali.
Ad oggi, infatti, l'unico caso in cui METRO C è obbligata ad ottenere il consenso al trattamento dei dati personali dei propri lavoratori è rappresentato dalla raccolta di immagini e/o registrazioni effettuate per finalità promozionali, che esulano dalla gestione del rapporto di lavoro in senso stretto.

Metro C non tratta, invece, dati biometrici: infatti alla luce del riformato quadro normativo, non solo si è chiarito il concetto di ***"dato biometrico"*** ma sono state tracciate delle linee di demarcazione più nette in ordine alla natura o meno di dato biometrico in relazione alle fotografie dei lavoratori, dei dipendenti, dei professionisti e dei consulenti di METRO C che vengono stampigliate sui tesserini di riconoscimento per l'accesso in sede ed in cantiere.

A norma del Considerando 51 del GDPR e degli interventi di interpretazione ad esso relativi forniti dalle Autorità Garanti, europea e nazionale, è stato chiarito che il trattamento di fotografie non costituisce sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di "dati biometrici" soltanto quando siano trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica: METRO C non esegue, infatti, né attività di riconoscimento facciale né fa uso di impronte digitali. La fotografia stampigliata sul tesserino di riconoscimento fornito da Metro C ed accompagnata dall'indicazione del nome, del cognome e della denominazione del Sub-affidatario presso cui il lavoratore è assunto ha il ben più limitato scopo di consentire agli incaricati del servizio di guardiania di verificare la corrispondenza del nominativo ivi presente con l'identità del suo portatore. Tale verifica, indispensabile ad appurare la legittimazione del presentatore ad accedere alla sede ed ai cantieri, è, a sua volta, strumentale all'adempimento da parte di Metro C dei propri compiti, imposti per legge, di sorveglianza e monitoraggio degli accessi per finalità di sicurezza di coloro che, a vario titolo, vi accedono (soprattutto lavoratori, ma anche fornitori, consulenti, visitatori) e del proprio patrimonio.
In conclusione, le fotografie stampigliate sui predetti tesserini NON assurgono a dati biometrici ma restano semplici dati personali comuni, il cui trattamento è lecito per la sussistenza delle riferite basi giuridiche.

d. ***Dati giudiziari***

riferibili alle persone fisiche operanti nell'ambito di METRO C S.c.p.A., 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 e ciò in attuazione dei protocolli d'intesa stipulati da Metro C con Roma Metropolitane e la Prefettura di Roma, per la prevenzione e il contrasto dei fenomeni di criminalità organizzata.
In generale, si rammenta che secondo la regola posta dall'art. 10 del Regolamento, il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

La norma eccezionale che legittima tale trattamento da parte di METRO C è contenuta nell'art. 2-octies, comma 3, del vigente Codice Privacy e precisamente nelle lettere a), c), h), i) ed m), ossia perché funzionale:

1. all'adempimento di obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di **diritto del lavoro** o comunque nell'ambito dei rapporti di lavoro;

2. la verifica o l'accertamento dei **requisiti di onorabilità**, requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;

3. l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni **antimafia** (e, segnatamente dal Codice Antimafia introdotto con D. Lgs. n. 159/2011) o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto;

4. l'accertamento del requisito di **idoneità morale** di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti;

> *m)* l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di **riciclaggio** dei proventi di attività criminose e di finanziamento del terrorismo.

Nel Parere relativo al trattamento di dati giudiziari effettuato da privati in attuazione dei Protocolli d'intesa stipulati per la prevenzione e il contrasto dei fenomeni di criminalità organizzata reso il 22 luglio 2021 (docweb 9693175), l'Autorità Garante ha preso atto che i dati relativi a condanne penali, a reati e alle connesse misure di sicurezza, trattati in attuazione dei menzionati Protocolli di intesa, possono essere raccolti e utilizzati, sulla base dell'art. 6, par. 1, del Regolamento, in presenza dei presupposti normativi sopra richiamati e nei limiti previsti dalle specifiche discipline vigenti in materia (art. 5, par. 1, lett. a) del Regolamento). In particolare, in ossequio alle prescrizioni ivi contenute, per il trattamento di tali dati personali Metro C osserva le seguenti regole:

- i dati raccolti e trattati in attuazione dei Protocolli di legalità sottoscritti fra Metro C, Roma Metropolitane e la Prefettura di Roma, sono adeguati, pertinenti e strettamente necessari alle finalità di prevenzione e contrasto dei fenomeni di criminalità organizzata (art. 5, par. 1, lett. c) del Regolamento;

- i dati trattati nell'ambito dei menzionati Protocolli sono esatti e aggiornati e non possono essere utilizzati per finalità diverse da quelle indicate, né trattati in operazioni non compatibili con le medesime finalità (art. 5, par. 1, lettere b) e d) del Regolamento);

- i dati devono riferirsi a soggetti/interessati specificamente individuati (artt. 85 e 91, comma 7, del d.lgs. n. 159/2011; art. 1, comma 53, della l. 190/2012);

- i princìpi di protezione dei dati, tra cui la minimizzazione, sono attuati in modo efficace fin dalla progettazione di applicazioni, servizi e prodotti (e di tali necessità si è tenuto in particolare conto nella recentissima attività di aggiornamento dei sistemi informativi della Società);

- possono essere trattati, per impostazione predefinita, solo i dati necessari per le specifiche finalità di trattamento (art. 25 del Regolamento).

5. ***Videoriprese***

Metro C svolge attività di foto e videoripresa dei propri cantieri per finalità promozionali.
Le attività di rilevazione di immagini a fini promozionali avvengono attraverso web cam installate presso i cantieri con modalità che non rendono identificabili i soggetti ripresi: infatti, sono effettuate ad alta quota, senza possibilità di zoom. Ciò non consente, neppure indirettamente, l'identificazione del lavoratore in cantiere, il che conduce ad escludere l'applicabilità del Regolamento (si veda in proposito FAQ n. 16 dell'Autorità Garante, V. 1.0 di dicembre 2020, per la quale *"la normativa in materia di protezione dati non si applica al trattamento di dati che non consentono di identificare le persone, direttamente o indirettamente, come nel caso delle riprese ad alta quota (effettuate, ad esempio, mediante l'uso di droni)"*.
Per la stessa motivazione, è esclusa altresì qualunque possibilità di controllo a distanza dell'attività dei lavoratori.
Tuttavia, a fini prudenziali ed in ottica di massima prevenzione, nei cantieri in cui la quota delle riprese non raggiunge altissime elevazioni, al fine di scongiurare ogni eventuale ipotetico rischio di identificabilità dei lavoratori, si è adottato un sistema software in grado di oscurare volti e targhe dei veicoli in cantiere.
In ogni caso, pur nell'inapplicabilità a monte del Regolamento, sempre in ottica di massima prevenzione, Metro C ha provveduto a:

- sottoscrivere un apposito Accordo con le competenti Rappresentanze sindacali (sebbene, come detto, non sussista alcuna possibilità di controllo a distanza dei lavoratori);
- rendere l'informativa agli interessati che, sul posto è affissa prima dell'accesso alla zona videosorvegliata ed è data in forma sintetica secondo il modello predisposto dall' EDPB mentre sul sito, a cui quella sintetica rimanda, è resa in forma estesa;
- individuare nei legittimi interessi perseguiti dal titolare del trattamento Metro C l'idonea base giuridica del trattamento in oggetto (articolo 6, paragrafo 1, lettera f), GDPR); legittimi interessi che, secondo l'orientamento espresso dall'EDPB nelle *"Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video",* versione 2.0, adottate il 29 gennaio 2020, possono avere natura giuridica, economica o immateriale – come nel presente caso);
- analizzare gli interessi coinvolti, al fine di verificare se sui propri legittimi interessi potessero prevalere o meno gli interessi o i diritti e le libertà fondamentali degli interessati. In considerazione dell'impossibilità di identificare, neppure indirettamente, i lavoratori in cantiere, non sono emersi loro interessi da contro-bilanciare;
- escludere, in ogni caso, l'impiego di qualunque tecnologia di riconoscimento facciale e/o di profilazione.

6. ***Social media e sito internet***

METRO C S.c.p.A. si avvale di ***social networks*** per scopi divulgativi e informativi e di un proprio sito internet istituzionale.
In relazione ai primi, METRO C S.c.p.A. è attiva sui principali network, tra cui Instagram e Twitter, ai quali l'utente può accedere tramite il sito istituzionale di METRO C mediante un apposito banner collocato nella pagina principale: su tali piattaforme vengono pubblicate delle fotografie e dei video a scopi divulgativi che consentono agli utenti di avere una visione storica delle attività di cantiere ed i progressivi sviluppi nella realizzazione dell'opera. Non vengono riprese persone fisiche identificate o identificabili.
In relazione al secondo, il **sito internet** istituzionale è predisposto a fini di conoscibilità e visibilità dell'opera e del Contraente Generale. Anche su esso vengono pubblicate fotografie e video, sempre per scopi divulgativi e memoria storica, i cui contenuti possono essere realizzati attraverso due distinte modalità.

Una prima, più sistematica, attraverso l'uso delle videocamere installate permanentemente presso i cantieri, secondo le modalità precedentemente indicate, ad una quota tale da non consentire l'identificazione del personale al lavoro, in ossequio a quanto previsto dalla Legge n. 300/1970. Come detto, si ricorda, inoltre, che laddove la quota di ripresa è stata ritenuta modesta, al fine di scongiurare ogni rischio di ripresa di lavoratori identificati o identificabili all'atto di svolgimento delle loro mansioni, Metro C ha predisposto l'adozione di uno specifico software che consente l'oscuramento di persone a mezzo busto e di veicoli. In ogni caso, presso i cantieri oggetto di ripresa, le zone videosorvegliate sono adeguatamente segnalate attraverso l'informativa semplificata predisposta dall'EDPB che rimanda all'informativa estesa contenuta sul sito istituzionale, presso cui i contenuti foto e video vengono pubblicati.
In alternativa, i contenuti pubblicati sul sito istituzionale di Metro C, possono essere realizzati ad hoc, nell'ambito di specifiche iniziative promozionali. In tale secondo contesto, la partecipazione dei lavoratori (per zone di ripresa limitate e per tempi ristretti) avviene previo avviso e su base volontaria. In tale secondo caso, ad essi vengono fornite l'apposita informativa estesa, richiesta una specifica liberatoria per la pubblicazione on line e prestato il consenso. Il mancato consenso del lavoratore non ne permette la partecipazione all'attività promozionale senza alcuna conseguenza per il lavoratore stesso.
Talvolta, sempre a scopi promozionali e divulgativi, i contenuti (essenzialmente foto e video, con possibilità di ulteriori informazioni in sovraimpressione, ad es. qualifica rivestita dal soggetto, accompagnata da nome e cognome, nell'ambito di interviste e/o iniziative specifiche) pubblicati sul sito istituzionale di Metro C vengono condivisi, per l'ulteriore loro pubblicazione, con le altre società, socie di Metro C o appartenenti al medesimo Gruppo imprenditoriale, che offrono garanzie di sicurezza ed affidabilità.
Il sito internet istituzionale di Metro C fa uso di **cookie**, dell'esistenza dei quali l'utente viene informato immediatamente, prima ancora di iniziare la navigazione, mediante apposito banner automatico che, con linguaggio chiaro e semplice, ne illustra le caratteristiche.
In particolare, Metro C si limita all'utilizzo di:

- ***cookie tecnici***, ossia solo di quelli impiegati all'esclusivo fine di *"effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio"* (cfr. art. 122, comma 1 del Codice);

- ***cookie analytics prime e terze parti*** equiparabili ai cookie tecnici perché, in relazione al sito istituzionale di Metro C, vengono utilizzati unicamente per produrre statistiche aggregate inerenti al solo proprio sito internet ; viene mascherata, per quelli di terze parti, almeno la quarta componente dell'indirizzo IP e le terze parti si astengono dal combinare i cookie analytics, così minimizzati, con altre elaborazioni (file dei clienti o statistiche di visite ad altri siti, ad esempio) o dal trasmetterli ad ulteriori terzi.

Metro C NON fa, invece, uso di cookie di profilazione, ossia di quelli utilizzati per ricondurre a soggetti determinati, identificati o identificabili, specifiche azioni o schemi comportamentali ricorrenti nell'uso delle funzionalità offerte (pattern) al fine del raggruppamento dei diversi profili all'interno di cluster omogenei di diversa ampiezza, in modo che sia possibile al titolare, tra l'altro, anche modulare la fornitura del servizio in modo sempre più personalizzato al di là di quanto strettamente necessario all'erogazione del servizio, nonché inviare messaggi pubblicitari mirati, cioè in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete.
L'utilizzo dei cookies è stato oggetto di apposita delibera dell'Autorità Garante del 10 giugno 2021 (Provvedimento n. 231, pubblicato in GU n. 163 del 9 luglio 2021) che ne ha approvato le relative linee guida, i cui contenuti erano già rispettati da METRO C che, nell'elaborazione della prima edizione del presente modello, si è ispirata al principio di massima prevenzione. In particolare, il sito istituzionale di

Metro C è strutturato in modo tale da rispettare le seguenti condizioni, in ossequio alle prescrizioni contenute nel citato provvedimento:

- utilizzando solo cookie tecnici e cookie analytics equiparati, non è richiesta l'acquisizione del consenso;
- l'utilizzo di tali cookie viene indicato nell'informativa;
- l'informativa è resa con linguaggio semplice ed accessibile; fruibile, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari;
- pur utilizzando solo cookie tecnici e cookies analytics equiparati (che legittimerebbe la collocazione della relativa informazione nella home page del sito o nell'informativa generale) Metro C, al fine di garantire la propria massima trasparenza e considerati gli usi ed i costumi della società dell'informazione, utilizza comunque un banner a comparsa immediata e di adeguate dimensioni che contiene:

    a) l'indicazione che il sito utilizza cookie tecnici e analytics equiparati;
    b) il link alla privacy policy contenente l'informativa completa, inclusi gli eventuali altri soggetti destinatari dei dati personali, i tempi di conservazione dei dati e l'esercizio dei diritti di cui al Regolamento;
    c) l'avvertenza che la chiusura del banner (ad es. mediante selezione dell'apposito comando contraddistinto dalla X posta al suo interno, in basso a destra) comporta il permanere delle impostazioni di default e dunque la continuazione della navigazione in assenza di cookie.

Alla data di approvazione del presente Modello, la Società sta predisponendo nuove modalità di funzionamento della **newsletter** che, ad oggi, consente – previa informativa, rilascio del consenso e possibilità di iscrizione e cancellazione di paritetica facilità – l'invio bimestrale di materiale informativo sull'andamento dei lavori e sulle caratteristiche dell'opera a coloro che hanno aderito. Ad oggi, la Società sta valutando nuovi contenuti, nuovi mezzi e nuove modalità di funzionamento di tali attività divulgative e promozionali.

"COME'"

In relazione al *"come"* i dati personali vengono trattati, in armonia con i principi di responsabilizzazione e di approccio basato sul rischio posti dal GDPR, all'interno di Metro C riveste particolare importanza la giusta ed equilibrata percezione del ***"peso" del dato personale***, stante l'assunto che non tutti i dati personali siano uguali e che, pertanto, non tutti debbano essere protetti allo stesso modo: a titolo esemplificativo, un dato relativo alla salute è più delicato di altri e, conseguentemente, METRO C S.c.p.A. ha ideato ed applicato un sistema di protezione più solido, costituito da regolamentazioni più rigide.

Sotto tale profilo, un ruolo cruciale rivestono la **cifratura dei dati** e la **pseudonimizzazione**, due misure di sicurezza che si rivelano preziose soprattutto in caso di attacco agli archivi o in occasione di *data breach*, smarrimento o furto dei dispositivi e altre fuoriuscite non volute di informazioni, che si pone in pratica sia quando il trattamento avviene con strumenti cartacei che con strumenti informatici.

Ogni Funzione di METRO C S.c.p.A. tratta i dati personali, come sopra elencati, limitatamente alla propria sfera di competenza, come definita dall'organigramma aziendale.

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.
A tutto il personale di Metro C vengono periodicamente impartite attività formative ed informative e, con il supporto della funzione DPO, le attività consulenziali inerenti a singoli casi concreti e/o quesiti specifici costituiscono occasione per la formazione e l'informazione reciproca continua.

Quando gestiti in ***forma elettronica***, i dati ed i relativi documenti vengono trattati mediante *personal computers*, fissi e 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 e dall'Amministratore del sistema. Nel caso di utilizzo di un PC diverso dal proprio, ogni incaricato deve, comunque, ricollegarsi alla rete con le proprie credenziali.
Tutta la gestione elettronica dei dati avviene sotto la responsabilità di METRO C che, in occasione delle rilevanti attività di aggiornamento e riorganizzazione dei sistemi informativi, ha adottato l'**applicativo SAP**, operante secondo i più recenti ed evoluti standards di sicurezza, che al momento dell'approvazione della presente seconda edizione vede completato il proprio iter di migrazione e che è giunto alla fase finale di testing prima del distacco completo dalla pregressa infrastruttura informatica. Alla descrizione dell'applicativo, delle funzionalità e delle misure di sicurezza ad esso connaturato è dedicata un'apposita sezione del presente modello, cui si rimanda.
Tale recente implementazione, che ha determinato la necessità di una nuova valutazione dei rischi privacy cui METRO C è esposta – si pone come punto finale di un più ampio processo generale che si è caratterizzato dalla programmazione, sin dal 2020, e dalla completa realizzazione, nel 2021, di un sistema di produzione e gestione dei documenti informatici di tipo contabile per la tenuta del protocollo informatico, della gestione dei flussi documentali, degli archivi e della conservazione elettronica: attraverso l'adesione al sistema di **conservazione sostitutiva** METRO C ha analizzato e disciplinato le attività di creazione, acquisizione, registrazione, classificazione e archiviazione dei documenti informatici al fine perseguire la massima reperibilità possibile e la trasparenza dei documenti contabili e fiscali.

Alle piattaforme aziendali hanno accesso il Personale dipendente di METRO C S.c.p.A. nonché le Società, i Professionisti ed i Consulenti esterni dalla stessa nominati Responsabili del trattamento ai sensi dell'art. 28 del GDPR, ai quali il Titolare del trattamento METRO C S.c.p.A. ha imposto il rispetto della riservatezza fin dall'atto della nomina, se non già tenuti per legge al rispetto del segreto professionale.
Le credenziali di autenticazione alle piattaforme informatiche vengono fornite direttamente dal Titolare del trattamento METRO C S.c.p.A.
Tutte le credenziali di accesso sono custodite da ciascun utente con la massima attenzione e, in caso di loro furto o smarrimento, è previsto il coinvolgimento immediato del Responsabile della Protezione dei Dati Personali (DPO) nominato da METRO C S.c.p.A. ai sensi dell'art. 37 del Regolamento UE 679/2016 il quale, senza indugio, richiede l'immediato intervento dell'Amministratore di sistema affinché blocchi le credenziali oggetto di furto e/o smarrimento, verifichi l'assenza *medio tempore* di eventuali accessi non autorizzati e fornisca nuove credenziali di autenticazione.
Al primo accesso da parte dell'incaricato, le credenziali vengono modificate a sua cura e sotto la sua esclusiva responsabilità.

Il sistema informatico è gestito da un **Amministratore di Sistema** nominato da Metro C, la cui nomina ed il cui relativo ambito di attività si conformano alle seguenti regole:

- l'attribuzione della funzione all'attuale Amministratore di Sistema, a seguito della rilevante modifica organizzativa di aggiornamento e potenziamento del sistema informatico che oggi è gestito autonomamente da Metro C, è avvenuta in continuità con il passato, avendo valutato l´esperienza, la capacità e l´affidabilità del soggetto designato, il quale ha fornito idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;
- la designazione è avvenuta con atto di nomina individuale, recante altresì l´elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- la Società conserva in un documento interno periodicamente aggiornato gli estremi identificativi delle persone fisiche amministratori di sistema, con l´elenco delle funzioni ad essi attribuite;
- Metro C, nella qualità di datore di lavoro, rende conoscibile ai propri lavoratori l'identità degli amministratori di sistema avvalendosi, in generale, dell'informativa a loro resa ai sensi dell'art. 13 GDPR e, nello specifico, mediante l'intranet aziendale;
- l'Amministratore di Sistema riferisce del suo operato ai vertici di Metro C con cadenza annuale;
- gli accessi logici eseguiti con le credenziali di Amministratore di Sistema vengono registrati;
- l'Amministratore di Sistema cura che con cadenza almeno annuale sia effettuato un *vulnerability assessment e penetration test* dell'intera infrastruttura informatica. Sempre in ottica di massima prevenzione, Metro C sottoscrive appositi contratti di servizi con aziende specializzate per l'esecuzione del *vulnerability assessment* e del *penetration test* ogni sei mesi.

Qualora sia necessario o strumentale per l'esecuzione delle specifiche finalità, i dati personali, oltre che dal personale interno di METRO C S.c.p.A., sono comunicati a destinatari designati **Responsabili del trattamento** ai sensi dell'art. 28 del GDPR, appartenenti alle seguenti categorie:

- Società *Partners*;
- Soggetti che forniscono servizi per la gestione del sistema informativo e delle reti di comunicazione di METRO C, ivi compresa la posta elettronica ed il sito internet;
- 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 gestori di reti stradali ed Autostradali;
- La Società Committente Roma Metropolitane;
- 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 METRO C S.c.p.A. e sui suoi portali informatici. In nessun caso i dati raccolti da METRO C S.c.p.A. sono oggetto di diffusione e/o di trasferimento all'estero, né all'interno né all'esterno dell'Unione Europea.
Nel rispetto di quanto previsto dall'art. 5, comma 1, lett. e) del GDPR, i dati personali vengono conservati in una forma che consente 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.

"CHI"

4. TITOLARI, RESPONSABILI E INCARICATI

Le figure e le funzioni coinvolte in METRO C S.c.p.A. nelle attività di protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale sono diversificate, a seconda dei singoli rapporti in cui i singoli trattamenti di inseriscono.

4.1 TITOLARE DEL TRATTAMENTO.

Di norma è la stessa società METRO C S.c.p.A. che riveste tale ruolo e sulla quale, conseguentemente, incombono tutti gli obblighi e le responsabilità che la legge, italiana ed europea, le impone. Primi fra tutti, l'obbligo di mettere in atto, riesaminare ed aggiornare le misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è da essa effettuato conformemente al Regolamento ed al D. Lgs. n. 196/2003, nella versione attualmente vigente e di rendere l'informativa ai soggetti interessati.

In particolare, METRO C è titolare del trattamento rispetto ai dati personali dei propri lavoratori, dipendenti e non, collaboratori, consulenti, anche esterni, e membri che rivestono cariche sociali o incarichi, con i quali intrattiene rapporti contrattuali per la prestazione dei servizi loro demandati.

Come accennato in precedenza, in virtù delle norme contenute nel Codice Antimafia e nei Protocolli di legalità sottoscritti fra Metro C, Roma Metropolitane e la Prefettura di Roma, Metro C è tenuta a sottoporre tali soggetti alle prescritte verifiche Antimafia ed al tracciamento dei flussi finanziari affinché sia garantita l'affidabilità e la legalità di azione di tutti i soggetti che, a vario titolo, vengono coinvolti nella più ampia attività di realizzazione dell'opera.

Le basi giuridiche sulle quali si fonda il trattamento sono rappresentate dall'esecuzione di un contratto di cui l'interessato è parte, dall'adempimento di un obbligo di legge cui METRO C è tenuta quale datore di lavoro ed il consenso (limitatamente allo svolgimento di attività non strettamente attinenti all'esecuzione del rapporto, come le attività promozionali cui si è fatto cenno in precedenza).

In relazione alle attività di trattamento che effettua nella qualità di titolare e direttamente per proprio conto, Metro C ha istituito ed aggiorna periodicamente un apposito **Registro delle attività di trattamento**.
In generale, si tratta dello strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti gli operatori, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo.
Nello specifico, Metro C ha adottato una modalità di compilazione elettronica, che consente una più agevole e costante attività di aggiornamento: trattandosi, infatti, di un documento di censimento e analisi dei trattamenti effettuati da Metro C è indispensabile che il suo contenuto corrisponda all'effettività dei trattamenti posti in essere.
Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, viene immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.
Il file, unico, viene gestito ed alimentato a cura del settore Risorse Umane che, in base alle attività di analisi e valutazione svolte, è risultato essere quello maggiormente interessato dal trattamento di dati personali appartenenti a categorie particolari di cui all'art. 9 del GDPR, soprattutto riferiti ai lavoratori.

Quanto al regime di responsabilità, METRO C S.c.p.A. risponde quale Titolare, in via solidale per l'intero ammontare, del danno materiale o immateriale cagionato a qualunque interessato da una violazione del GDPR, salvo che dimostri che l'evento dannoso non gli è in alcun modo imputabile.

4.2 RESPONSABILE DEL TRATTAMENTO.

Il GDPR definisce all'art. 28 il Responsabile del trattamento come il soggetto che effettua trattamenti di dati personali per conto del Titolare, presentando garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che i trattamenti stessi soddisfino i requisiti del GDPR e garantiscano la

tutela dei diritti dell'interessato.

METRO C ha provveduto, già all'indomani della prima edizione del presente modello, alla nomina dei propri **Responsabili del trattamento**, secondo due distinte modalità: per coloro i quali, alla data di piena operatività del Regolamento, avevano già in corso trattamenti di dati personali effettuati per conto di METRO C, quest'ultima ha provveduto alla designazione in parola mediante un *addendum* ai contratti già in essere mentre, in relazione ai nuovi contratti conclusi successivamente a tale data, la designazione è stata integrata all'interno del testo contrattuale.

Le attuali categorie di Responsabili del trattamento designati da METRO C sono:

7. la Committente Roma Metropolitane S.r.l.;
8. il Direttore dei Lavori, il Responsabile dei Lavori, il CSE/CSP;
9. l'Internal Auditing;
10. gli Avvocati;
11. il Consulente del Lavoro;
12. i Consulenti Assicurativi;
13. il Consulente della comunicazione;
14. la Società di Revisione;
15. gli altri Consulenti esterni che gestiscono dati personali per conto di METRO C.

L'elenco analitico, contenente gli estremi identificativi dei singoli Responsabili, è aggiornato periodicamente ed è conservato a cura della Società presso la propria sede.

METRO C, inoltre, assume essa stessa il ruolo di responsabile del trattamento in relazione ai dati personali di titolarità di soggetti terzi, essenzialmente suoi sub-affidatari, in relazione ai dati del personale di cantiere che il sub-affidatario stesso impiega per la realizzazione delle opere.
In sostanza, il personale di cantiere (che rappresenta la figura dell'interessato) è assunto alle dipendenze di ciascun singolo sub-affidatario (che assume il ruolo di titolare del trattamento) il quale trasmette i dati dei singoli lavoratori, inerenti soprattutto alla rilevazione delle presenze in cantiere, indispensabili a METRO C per assolvere ai doveri ad essa imposti per legge in materia di igiene e sicurezza sul lavoro e dalla normativa Antimafia sopra richiamata.
A tal proposito, METRO C, facendosi parte diligente, ha segnalato alle proprie controparti-Titolari del trattamento la necessità di essere designato Responsabile ai sensi dell'art. 28 GDPR, all'occorrenza fornendo indicazioni e modelli di base standardizzati, da personalizzare a cura del Titolare del trattamento a seconda delle singole esigenze concrete.

Anche in relazione alle attività di trattamento per le quali agisce in qualità di Responsabile del trattamento, Metro C ha predisposto uno specifico Registro delle attività e, come nel caso del Registro predisposto in qualità di Titolare esaminato nel paragrafo precedente, ne è stata prescelta una modalità compilazione elettronica, funzionale ad agevolare le attività di periodico aggiornamento ed implementazione; ma a differenza di quello – che è caratterizzato da un singolo ed unico file – nel caso in esame la sua composizione è suddivisa in tanti files quanti sono i sub-affidatari, oltre una parte generale comune caricata sulla Piattaforma Sharepoint nella stanza del DPO. Tale scelta è stata necessitata dalla constatazione che agendo Metro C in qualità di responsabile del trattamento per conto di più Sub-Affidatari quali autonomi e distinti titolari, le informazioni di cui all'art. 30, par. 2 del RGPD devono essere riportate nel registro con riferimento a ciascuno dei suddetti titolari.

Quanto al regime di responsabilità, in generale, i Responsabili del trattamento rispondono per il danno causato dal trattamento solo se non hanno adempiuto gli obblighi del GDPR specificatamente loro diretti o se hanno agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare del trattamento.
Sono altresì esonerati dalla responsabilità per danni se dimostrino che l'evento dannoso non è in alcun modo loro imputabile. Rispondono, inoltre, delle sanzioni amministrative pecuniarie irrogabili dall'Autorità Garante secondo gli stessi termini e modalità del Titolare del Trattamento.

Infine, benché non espressamente prevista ma certamente non vietata dalla normativa, METRO C ha istituito al proprio interno, sin dal 2018, la figura del **Responsabile *"interno"* del trattamento** volta a garantire l'applicazione e la vigilanza effettive e capillari delle norme del GDPR, all'interno di singoli aree e settori ritenuti chiave.
In particolare, i Responsabili "interni" del trattamento hanno funzioni di direzione, coordinamento e vigilanza sugli incaricati sottoposti che, materialmente, procedono ai trattamenti. Tali figure vengono nominate, una per ciascun settore ritenuto sensibile, sulla base di un contratto, il cui facsimile è stato già allegato alla prima versione del presente Modello, composto da una sezione generale indifferenziata e da una speciale, distinta per singolo settore, al fine di tener conto delle singole specificità ed esigenze di tutela dei dati concretamente trattati per ciascun settore.

I Responsabili interni dei trattamenti attualmente individuati sono i referenti delle seguenti funzioni:

1. Acquisti, contrattualistica e Protocollo di legalità;
2. Amministrazione, Finanza, Risorse Umane, Servizi Generali e Sistemi Informativi;
3. Legale;
4. RSGI (Sistema Integrato Qualità, Sicurezza, Ambiente).

4.3. PERSONE AUTORIZZATE AL TRATTAMENTO.

Le *persone autorizzate al trattamento dei dati personali* sono coloro che, *sotto l'autorità diretta del Titolare o del Responsabile*, compiono materialmente le attività di trattamento dei dati personali (che non implicano soltanto l'elaborazione del dato e la sua modifica ma comprendono anche la semplice possibilità di visualizzazione del dato stesso) e che, sotto la previgente normativa, erano definiti "incaricati del trattamento".

METRO C S.c.p.A., prima ancora che tali soggetti inizino le attività di trattamento, provvede a nominarle, istruirle e vincolarle alla riservatezza: in particolare, le attività formative ed informative vengono somministrate alle persone autorizzate ai trattamenti sia all'inizio del loro rapporto con METRO C sia periodicamente mediante apposite attività di aggiornamento che, ancora, su necessità anche *"one-to-one"* mediante l'intervento del Responsabile della Protezione dei dati personali (DPO).

5. FUNZIONI E PROCESSI INTERESSATI – ORGANIGRAMMA PRIVACY

Nel dettaglio, si illustrano le categorie di dati personali trattati dalle singole funzioni:

16. 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.

Come accennato, il trattamento dei dati di cui al punto b) è funzionale all'adempimento degli obblighi previsti dalla normativa Antimafia (D. Lgs. 6 settembre 2011, n. 159, modificato dal D. Lgs. 15 novembre 2012, n. 218, dal D. Lgs 13 ottobre 2014, n. 153 e dalla Legge 6 agosto 2015, n. 121) e dal Codice degli Appalti, cui METRO C S.c.p.A. è tenuta in qualità di Contraente Generale.

17. La funzione **Amministrazione e finanza, Risorse Umane e Servizi Generali** tratta 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. 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 METRO C derivanti dalla legge o dal contratto individuale nonché l'esatto adempimento della prestazione e commisurare l'importo della retribuzione;

c. 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.

18. **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. fotografie dei lavoratori, necessarie all'elaborazione dei tesserini di riconoscimento per l'accesso in sede ed in cantiere.

19. Le funzioni di **Direttore Generale e Amministratore Delegato** sono Funzioni apicali e di raccordo tra tutte le altre funzioni Aziendali sottoposte e con le quali interloquiscono; il Direttore Generale e l'Amministratore Delegato hanno accesso a tutte le categorie di dati personali trattati da METRO C S.c.p.A., 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.

20. **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, soprattutto se implicanti l'uso di gru, veicoli di movimento terra o, in genere, di macchinari caratterizzati da alto livello di pericolosità;

c. fotografie dei lavoratori, necessarie all'elaborazione dei tesserini di riconoscimento per l'accesso in cantiere ed in sede.

21. **Il Coordinatore per la sicurezza in fase di progettazione ed esecuzione (CSP/CSE)** 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. fotografie dei lavoratori stampigliate sui tesserini di riconoscimento per l'accesso in cantiere.

22. **L'Ufficio di Comunicazione** gestisce:

a. i dati personali utili alla realizzazione e alla gestione dei contenuti diffusi tramite i social media, il sito internet della società e talora, come detto, condivisi con i propri Partners (essenzialmente Webuild, per il tramite della società Partecipazioni Italia). Il trattamento dei dati si esplica nella gestione di foto degli apicali della società inserite sul sito e la gestione di materiale fotografico di manifestazioni ed eventi pubblici con lo scopo di divulgare tali informazioni all'opinione pubblica relativamente allo

stato di avanzamento dei lavori. Detto Ufficio provvede, altresì, alla gestione dei contenuti video realizzati come sopra specificato;

b. i dati personali dei visitatori (nome, cognome, qualifica, data della visita) a cui viene sottoposta l'informativa, raccolto il consenso al trattamento dei dati personali ove coinvolti in riprese foto/video e rilasciata la liberatoria per la pubblicazione on line delle riprese e/o delle foto.

Come accennato, la raccolta di immagini, filmati e contenuti multimediali che vedano coinvolto il personale dipendente è preceduta da apposita informativa, manifestazione del loro consenso e dalla specifica liberatoria rilasciata per la diffusione. In proposito, METRO C si attiene strettamente alle prescrizioni contenute nel provvedimento in materia di videosorveglianza emesso dal Garante con delibera del giorno 8 aprile 2010 e pubblicato in GU del 29 aprile 2010 n. 99 e precisamente:

- viene rispettato il divieto di controllo a distanza dell'attività lavorativa orientando le telecamere e gli apparecchi di ripresa quanto più distante possibile dai lavoratori e comunque ad una distanza tale da non consentirne l'identificazione;
- nelle aree site nelle immediate vicinanze di quelle interessate dalle riprese vengono affisse apposite segnalazioni, onde consentire al personale di conoscere in anticipo il raggio di azione delle telecamere.

23. **I Sistemi informativi** costituiscono il settore maggiormente colpito dal Regolamento in quanto tutti i dati gestiti dalle funzioni precedenti sono archiviati sulla nuova piattaforma SAP e, solo marginalmente fino al distacco definitivo, sulla piattaforma Sharpoint. Per quanto riguarda l'architettura e le misure di sicurezza dello stesso si rimanda alle sezioni 7-8-9.

La struttura organizzativa della Società ("**Organigramma privacy**") funzionale al trattamento dei dati è riepilogata nell'allegato 2 del presente modello.

6. RISK ASSESSMENT

Come anticipato nei capitoli precedenti, in occasione della prima edizione del presente Modello risalente al 2018, al fine di implementare le azioni volte all'adeguamento al Regolamento UE 679/2016 in materia di dati personali, è stata effettuata una ricognizione dell'organizzazione e della documentazione allora vigente in materia di privacy e delle misure tecniche utilizzate.
In particolare, si è proceduto, con l'ausilio di consulenti esterni, con l'esame della principale documentazione organizzativa e procedurale; alla luce di tale analisi, è stato predisposto uno specifico questionario finalizzato all'identificazione dei principali rischi di non conformità al Regolamento UE 679/2016.
Il suddetto questionario è stato compilato dai Responsabili "interni" del Trattamento, ai quali è stato richiesto di indicare *quali* dati fossero trattati e *come* venissero trattati nello svolgimento delle proprie attività. I questionari sono stati successivamente rivisti dalla funzione Internal Auditing e dagli Avvocati incaricati.
Sulla base delle informazioni e valutazioni riportate nonché dei presidi esistenti a mitigazione dei rischi identificati, è stata effettuata una prima valutazione sul livello di ***probabilità*** del rischio, **sull'*impatto economico*** eventualmente derivabile, sul **livello di *rilevabilità*** *del rischio* in relazione ai controlli preventivi effettuati.

Per la valutazione di tali rischi, è stata utilizzata una scala di valori su 5 livelli:

1 – Molto basso 2 – Basso 3 – Medio 4 – Medio Alto 5 – Alto

Nello specifico, in relazione alla valutazione della **probabilità** e dell'**impatto**, i valori di riferimento che sono stati individuati come **orientativi**, sono stati i seguenti:

Livello	Livello di Probabilità	Livello di Impatto
1= Molto Basso, con effetti trascurabili	probabilità ≤1%	impatto ≤10 mila €
2= Basso, con effetti limitati	1% < probabilità ≤5%	10 mila € < impatto ≤ 50 mila €
3= Medio, con effetti moderati	5% < probabilità ≤15%	50 mila € < impatto ≤ 200 mila €
4= Medio Alto, con effetti elevati	15% < probabilità ≤ 30%	200 mila € < impatto ≤ 1 milione €
5= Alto, con effetti molto significativi	probabilità > 30%	Impatto > 1 milione €

Relativamente alla valutazione della **rilevabilità** del rischio, invece, i principali elementi che sono stati considerati sono relativi a:

- procedure complete e formalizzate,
- adeguati controlli e relativa tracciabilità,
- responsabilità organizzative definite.

L'analisi dei rischi effettuata è stata di tipo auto – valutativo supportato da un'**analisi critica delle valutazioni espresse**, effettuata da consulenti esterni, attraverso il cui contributo è stato possibile effettuare un'analisi più aderente possibile alla società.
Per ciascun rischio, è stato individuato il **ranking di rischio (IPR),** calcolato sulla scorta delle seguenti variabili:

- **Rischio lordo**: media tra *probabilità* del rischio ed *impatto economico* eventualmente derivabile;
- **Rischio residuo netto**: Rischio lordo al netto del livello di *rilevabilità* del rischio.

Al fine di rappresentare in maniera sintetica gli esiti delle valutazioni di Risk Assessment svolte, è stata quindi costruita la **Matrice dei rischi** che riporta le valutazioni dei Rischi cui è esposta ciascuna funzione aziendale di riferimento.
Il colore di ciascuna cella è in funzione della valutazione del Rischio Lordo/ Residuo Netto, secondo una scala di valori che va da 1 a 5.

	Molto basso
	Basso
	Medio
	Medio alto
	Alto

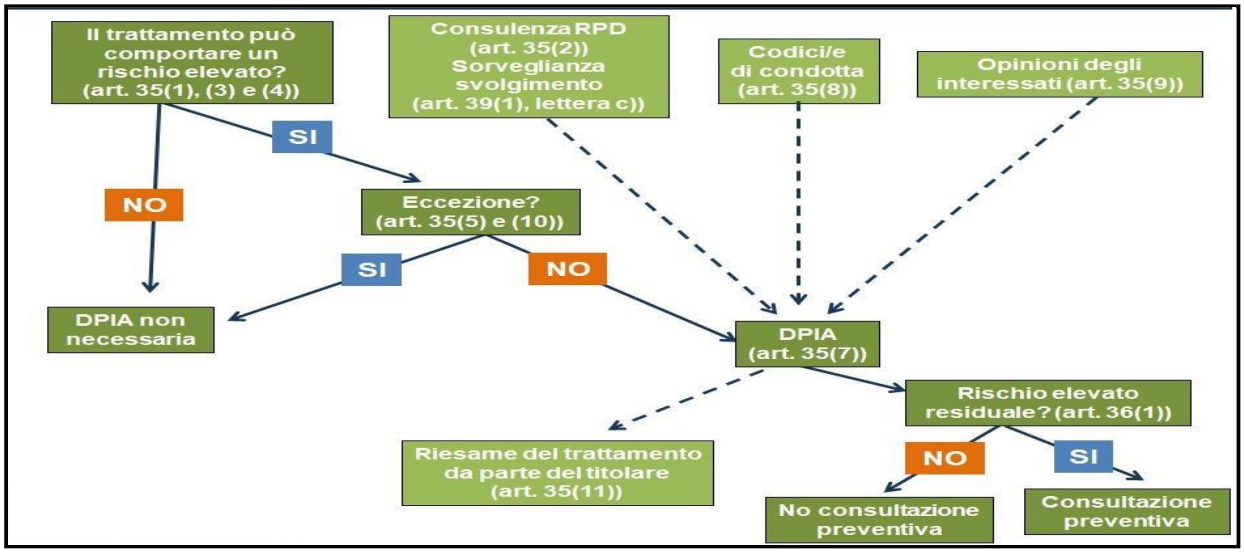
Sulla base dei possibili rischi individuati e delle valutazioni effettuate, di seguito l'elenco dei rischi con la relativa valutazione:

N.	Possibile rischio	Valutazione
1	Mancata/insufficiente informativa della finalità del trattamento	B
2	Ritenzione di dati eccedenti rispetto alle finalità	B
3	Trattamento non consentito o non conforme alle finalità della raccolta	B
4	Assenza/insufficienza del consenso espresso dall'interessato	B
5	Mancata indicazione di categorie particolari di dati personali	B
6	Inadeguato/mancato accesso ai dati personali da parte dell'interessato	B
7	Comportamento sleale/fraudolento nella raccolta/gestione/controllo dati	B
8	Comunicazione e diffusione dei dati non consentita	B
9	Modifica accidentale dei dati	B
10	Perdita/sottrazione di strumenti contenenti dati/ distruzione accidentale o illegale dei dati/eventi distruttivi/naturali o artificiali	B
11	Mancata cancellazione dei dati una volta finita la durata relativa al loro utilizzo	B
12	Inadeguato/mancato aggiornamento dei dati	B
13	Inadeguati/mancati presidi per il controllo dell'esattezza dei dati personali raccolti	MB
14	Inadeguata supervisione e presidio dei trattamenti dei dati (mancanza DPO)	B
15	Inadeguata/mancanza di controllo sull'archiviazione cartacea dei dati	B
16	Accessi non autorizzati a locali ad accesso riservato	B
17	Inadeguata/mancata conservazione dei dati relativi ai dipendenti in opportuni schedari chiusi e ad accesso riservato	B
18	Mancata evidenza della criptatura e paragdimizzazione dei dati	B

19	Inadeguata/mancata gestione di procedure/strumenti di password di accesso agli strumenti telematici/informatici	B
20	Sottrazione di credenziali di accesso	B
21	Malfunzionamento/indisponibilità di strumenti informatici	B
22	Virus informatici/spamming/intercettazioni	B
23	Inadeguata/mancata segnalazione di impianti di videosorveglianza	B
24	Mancato/inadeguato accordo di contitolarità del trattamento con le funzioni in outsourcing; inadeguata supervisione	B
25	Assenza/insufficienza di formazione del personale	B
26	Data Breach	B
27	Brand Reputation	B

Dall'analisi svolta sono stati così **mappati n. 27 rischi,** dai quali risultava nel 2018 un complessivo **rischio netto BASSO.**

Nell'attività di analisi dei rischi svolta già in sede di prima approvazione del presente Modello era stata esaminata la necessità o meno di effettuare una valutazione d'impatto con riferimento al trattamento dei dati che potesse *"presentare un rischio elevato per i diritti e le libertà delle persone fisiche"*. La valutazione preliminare è stata effettuata secondo il seguente schema:



Dall'analisi effettuata non era emersa l'esigenza di effettuare una dettagliata valutazione d'impatto (c.d. DPIA) in senso stretto, in quanto non era stata rilevata neppure allora alcuna delle condizioni di cui *al comma 1* né alle *lettere a), b) e c), comma 2, dell'art. 25* del GDPR: METRO C S.c.p.A., infatti, non solo non faceva e non fa tutt'ora uso di nuove tecnologie per effettuare tipi di trattamento caratterizzato da un rischio elevato per i diritti e le libertà delle persone fisiche ma altresì non operava e non opera tutt'ora alcuna valutazione sistematica e globale di aspetti personali di persone fisiche basata su un trattamento automatizzato, non effettuava e non effettua tutt'ora trattamenti su larga scala di dati sensibili né sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Tali condizioni caratterizzano anche lo stato attuale, per il quale, dunque, non si rende neppure oggi obbligatoria l'esecuzione di una valutazione di impatto in senso stretto. Tuttavia, in ottica di continuo miglioramento tesa ad implementare periodicamente il sistema di controllo, si è ritenuto di:

- rinnovare l'individuazione dei rischi che, all'esito, ha consentito di confermare l'identificazione già a suo tempo svolta;
- analizzare nuovamente i livelli di rischio cui METRO C è esposta, alla luce del progetto di aggiornamento e riorganizzazione dei sistemi informativi della Società, in esito al quale è stato possibile rilevare un sensibile abbassamento del livello di rischio grazie al maggior livello di sicurezza che SAP offre rispetto a Sharepoint, soprattutto in relazione ai processi maggiormente impattati da tale modifica organizzativa;
- implementare la matrice dei rischi prendendo in considerazione, in modo analitico, anche quelli cui sarebbero potenzialmente esposti gli interessati a fronte di un'ipotetica violazione dei loro dati personali, con ciò consentendo di guardare al generale concetto di *"rischio"* sotto un duplice angolo visuale di esposizione: METRO C, da un lato, e gli interessati, dall'altro. Il che, nella sostanza, assolve alla medesima *ratio* di protezione dei diritti e delle libertà degli interessati cui è finalizzata la valutazione di impatto.

7. BANCHE DATI AZIENDALI E MODALITA' DI ARCHIVIAZIONE

[OMISSIS]

8. AREE, LOCALI, STRUMENTI DI TRATTAMENTO

Il trattamento dei dati avviene, con le modalità di seguito riportate, sia presso la sede legale ed operativa, situata in Via dei Gordiani snc a Roma sia in tutti i cantieri attivi o che apriranno in futuro (Tratta T3 e T2).
L'accesso all'edificio di via dei Gordiani è consentito anche al pubblico ed avviene da un'unica entrata, situata nella medesima via, sulla cui parete esterna è affissa l'informativa resa da METRO C ai sensi dell'art. 13 del Regolamento.
L'unica entrata è soggetta a presidio ininterrotto di guardiania, sia durante l'orario di lavoro che nelle ore notturne.
L'ingresso dei dipendenti, dopo il passaggio dal posto di guardiania, viene registrato dai badge situati all'interno di ogni edificio. Tale operazione si rende necessaria per la rilevazione delle presenze e la conseguente commisurazione delle spettanze dei dipendenti nonché per ragioni di sicurezza.
L'ingresso di visitatori esterni viene registrato, a cura del personale di guardiania, su un apposito registro cartaceo che, ogni due settimane viene consegnato in originale al DPO e sistematicamente scansionato ed archiviato sulla piattaforma informatica. Ciascun visitatore viene munito di un apposito modulo che viene controfirmato dal responsabile dei METRO C che riceve il visitatore.

Il trattamento dei dati personali dei visitatori, rappresentati da dati anagrafici e dall'indicazione degli orari di ingresso ed uscita avviene per motivi di sicurezza *[OMISSIS]*
Gli uffici sono protetti da sistema di allarme e l'edificio "E" nel quale è situata la sala server, è protetto anche con servizio di telesorveglianza. Le immagini sono conservate solamente per il tempo necessario al loro esame.
Nei cantieri l'acceso è consentito solamente agli addetti autorizzati. I cantieri sono presidiati da servizio di guardiania.
Anche presso i cantieri è affissa l'informativa

[OMISSIS]

I supporti cartacei, compresi quelli contenenti immagini, sono raccolti in schedari ubicati presso la sede, nei rispettivi uffici e collocati dentro armadi o stanze con chiusura a chiave ad accesso consentito solo alle persone autorizzate (v. lista incaricati).
In tali archivi sono conservati i documenti di comune e continuo utilizzo nonché quelli giunti a fine ciclo lavorativo. Tutti i documenti sono archiviati dal protocollo, scannerizzati ed archiviati informaticamente in allegato al data base del protocollo sulla Piattaforma SharePoint.
I documenti relativi al personale vengono direttamente consegnati all'Ufficio personale e da questo gestiti.
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 elaborazione;
2) i dati sensibili trattati sistematicamente con supporti cartacei e con elaborazione 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**
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.
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.
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.

Responsabile dei Lavori	Raccolta, organizzazione, conservazione, consultazione dei dati relativi al cantiere e al personale impiegato nell'esecuzione delle opere.
Coordinatore per la sicurezza in fase di progettazione ed esecuzione (CSP/CSE)	Raccolta, organizzazione, conservazione, consultazione dei dati relativi ai cantieri, agli appaltatori e subappaltatori ed al personale impiegato nell'esecuzione delle opere.
Comitato Tecnico	Esamina i dati inerenti la gestione tecnico-economico-finanziaria dei lavori. Dati relativi a: personale (organico, politiche retributive,gestione del personale), fornitori, affidatari, Ente Appaltante, Istituti di Credito, Compagnie di assicurazione e cauzione, OO.SS., consulenti esterni.
(RSGI) Sistema Integrato Qualità-Sicurezza-Ambiente	Gestisce 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. Gestione dei dati relativi agli appaltatori, consulenti esterni, dei dati contrattuali, dei dati relativi alla salute e sicurezza dei lavoratori.
Servizio Ingegneria	Il Responsabile della progettazione Preliminare, Definitiva, Esecutiva ed Esecutiva di Cantierizzazione coordina le attività espletate dalla propria struttura e dalla pluralità degli affidatari di servizi di progettazione che concorrono alla predisposizione delle varie fasi progettuali.
Amministrazione e Finanza Risorse Umane	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. 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 a Webuild / Deloitte - Gestione buste paga - Selezione e sviluppo del personale.

Servizi generali Sistemi informativi	Distribuzione di tutti i documenti amministrativi e della corrispondenza in entrata e in uscita Gestione di tutti i dati informatici
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, degli adempimenti amministrativi/legali relativi al protocollo di legalità.
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, esecuzione degli adempimenti antimafia di cui al D. Lgs. n. 159/2011 ("Codice Antimafia").
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.
Segreteria di Presidenza e dell'Amministratore Delegato	Raccolta, organizzazione, conservazione, consultazione, modificazione, utilizzo, comunicazione, cancellazione dei dati di competenza dell'AD. Raccoglie e gestisce archivio Metro C, gestisce ed implementa la PMC di tutti i documenti dell'AD.
Segreteria DG	Controllo dei documenti in entrata ed in uscita di competenza del DG/CM. Gestisce ed implementa la PCM della documentazione riferita ad appaltatori e subappaltatori/fornitori. Gestisce le RDA sulla PCM e nel relativo archivio cartaceo, nonché l'inoltro degli ordini agli affida-tari e la loro archiviazione sulla PCM.
Piattaforma Controllo e Monitoraggio	Gestione Sharepoint
Comunicazione	Raccolta, organizzazione, elaborazione, conservazione, consultazione, modificazione, utilizzo, comunicazione, diffusione, di dati relativi alla gestione della comunicazione di progetto.
Consulente assicurativo	Gestione dati relativi a Compagnie di assicurazione e cauzione, Istituti di credito.
Archivio generale	Raccolta, organizzazione, scannerizzazione, archiviazione, distribuzione di tutti i documenti amministrativi e della corrispondenza in entrata e in uscita.
Servizio	Archiviazione dei dati di accesso del personale,

Portineria	visitatori e collaboratori.

9. 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 di carattere generale:

● 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 ed antivirus centralizzati;
● prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili, contenenti dati personali.

[OMISSIS]

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