

PROCEDURA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI E DI SICUREZZA INFORMATICA

STATO DEL DOCUMENTO	Proposto ed emesso da:	Verificato da:
Identificazione: PO-18	DPO Erika Salvatore	Presidente Alessandro Lamberti
	Responsabile Sistemi Informativi Antonino Campo	
Approvata dal Consiglio di amministrazione in data 26 settembre 2025		

Lista delle modifiche			
Identificazione	Revisione	Data	Tipo di modifica
PO-18	0	10/05/2023	Prima emissione
PO-18/1	1	25/09/2025	Revisione

Sommario

1.	Introduzione.....	4
2.	Scopo.....	4
3.	Ambiti e destinatari.....	4
4.	Normativa di riferimento	4
5.	Definizione e acronimi.....	4
6.	Principi generali sulla protezione dei dati personali	7
6.1.	<i>Accountability</i>	7
6.2.	<i>Liceità, Correttezza, Trasparenza e Base giuridica del trattamento</i>	7
6.3.	<i>Limitazione della finalità e Minimizzazione dei dati</i>	8
6.4.	<i>Esattezza</i>	8
6.5.	<i>Limitazione della conservazione (data retention)</i>	8
6.6.	<i>Integrità e riservatezza</i>	8
6.7.	<i>Privacy by design e by default</i>	8
7.	Responsabilizzazione.....	9
7.1.	<i>Titolare del Trattamento</i>	9
7.2.	<i>Responsabile del Trattamento</i>	9
7.3.	<i>Data Protection Officer</i>	9
7.4.	<i>Amministratore di Sistema</i>	9
8.	Processi di Governance in materia di protezione dei dati personali	10
8.1.	<i>Informativa</i>	10
8.2.	<i>Gestione Diritti degli Interessati</i>	10
8.3.	<i>Gestione Terze parti e nomina dei responsabili esterni del trattamento</i>	11
8.4.	<i>Mappatura del Registro dei Trattamenti</i>	11
8.5.	<i>Gestione Data Breach</i>	11
8.6.	<i>Data Protection Impact Assessment</i>	11
9.	Le Misure di sicurezza ICT.....	12
9.1.	Disposizioni in merito alle modalità d'uso degli strumenti aziendali e verifiche	12
9.2.	Principi generali sulla sicurezza delle informazioni	12
10.	Formazione e Consapevolezza	13
11.	Sanzioni.....	13
12.	Modifiche e aggiornamenti.....	13
13.	Diffusione	14
14.	Altri Riferimenti e Disposizioni Finali	14
	Verifica Protocollo di Legalità e Autorizzazioni alla Contrattualizzazione	15

Videosorveglianza in Tempo Reale (senza registrazione).....	15
Sinistri Attivi e Passivi in Costruzione	15
Sicurezza dei Sistemi e Assistenza Tecnica IT	16
Gestione Ingressi Personale e Visitatori	17
Gestione degli ingressi del personale dipendente (incluso accesso biometrico)	17
Gestione Eventi	18
Adempimenti D.Lgs. 231/2001	18
Gestione Contenziosi (Dipendenti, Terzi, Societari)	18
Gestione degli Adempimenti Societari	19
Attività Pubblicitarie, Promozionali, Sponsorizzazione, Marketing, Comunicazione e Informazione – Tabella Retention....	19
Gestione del processo di esproprio e della liquidazione dell'indennità agli espropriati – Tabella Retention.....	20
Gestione del Personale e Recruiting	20
Gestione dei Collegamenti ai Social Network	21
Gestione del Ciclo Passivo (Fornitori e Professionisti).....	21
Gestione Carte Prepagate e Carte di Credito Aziendali	22
Accesso civico, accesso generalizzato e accesso agli atti.....	22
Sicurezza sul Lavoro e Gestione Infortuni.....	23

1. Introduzione

Il Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679), la cui piena applicazione ha avuto effetti a partire dal 25 maggio 2018, offre un quadro di riferimento in termini di compliance per la protezione dei dati in Europa, aggiornato e fondato sul principio di responsabilizzazione (accountability).

L'obiettivo è garantire un livello coerente e solido di protezione dei dati personali trattati nel contesto delle attività poste in essere, indipendentemente da dove tali attività possano aver luogo.

2. Scopo

SPV Linea M4 Spa (di seguito "M4"), ha deciso di adottare la presente procedura in materia di protezione dei dati personali e sicurezza IT per definire i principi e identificare il modello operativo per l'adempimento delle attività privacy e dei relativi processi di governance dei dati in proprio possesso.

3. Ambiti e destinatari

Tutti gli amministratori, i dirigenti, i dipendenti e i collaboratori di SPV Linea M4 S.p.A. (i "Destinatari") sono coinvolti nella presente procedura.

4. Normativa di riferimento

- Statuto della Società SPV Linea M4 S.p.A.;
- Codice Etico e di Comportamento di M4 S.p.A.;
- Modello di Organizzazione Gestione e Controllo di M4 S.p.A. ai sensi del D.lgs. 231/2001;
- Regolamento Generale sulla Protezione dei Dati n. 2016/679
- Codice in materia di Protezione dei Dati Personali D.Lgs. 196/2003
- Decreto legislativo 10 agosto 2018, n. 101 che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679

5. Definizione e acronimi

- **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
- **Amministratori di Sistema ("AdS"):** figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei Dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi
- **Categoria degli interessati:** Categoria di persone fisiche a cui fanno riferimento i dati trattati (es. dipendenti, fornitori, clienti retali, referenti di clienti B2B, prospect, ecc...)
- **Dati Biometrici:** i Dati Personali ottenuti da un Trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici

- **Dati Comuni:** sono tutti i Dati Personali che non appartengono alle categorie dei Dati Particolari e Dati Giudiziari
- **Dati Genetici:** i Dati Personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione
- **Dati Giudiziari:** Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza
- **Dati Particolari:** Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona
- **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
- **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
- **Destinatario/i:** 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
- **Device Fissi:** si intendono gli strumenti informatici non facilmente removibili dal perimetro aziendale quali personal computer, server locali, stampanti, affidati alle Persone Autorizzate per uso professionale
- **Device Mobili:** in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili dal perimetro aziendale quali chiavette USB, SD cards, hard disk esterni, tablet e smartphone, utilizzati dalla Persone Autorizzate per uso professionale
- **Finalità del Trattamento:** rappresenta il processo aziendale nell'ambito del quale è necessario effettuare uno o più trattamenti di dati personali
- **Funzioni Aziendali:** Direzioni/Funzioni Aziendali che effettuano il trattamento di dati personali della Società
- **GDPR o Regolamento:** Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679
- **Incaricato/i o Persona/e Autorizzata/e:** si tratta dei Collaboratori autorizzati al Trattamento dei Dati Personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4(10) e 29 del GDPR. Stante la definizione fornita dal Gruppo di Lavoro Articolo 29 dell'Opinione 2/2017 questa definizione ricomprende: dipendenti ed ex dipendenti, dirigenti, sindaci, collaboratori e lavoratori a partita IVA,

lavoratori a chiamata, part-time, job-sharing, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, nonché consulenti e fornitori della Società e, più in generale, tutti coloro che utilizzino od abbiano utilizzato Strumenti Aziendali o Strumenti Personali operino sulla Rete ovvero siano a conoscenza di informazioni aziendali rilevanti quali, a titolo esemplificativo e non esaustivo: (a) i Dati Personali di clienti, dipendenti e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura commerciale, finanziaria o di strategia di business; nonché (c) i dati e le informazioni relative ai processi aziendali, inclusa la realizzazione di marchi, brevetti e diritti di proprietà industriale, la cui tutela prescinde dagli effetti pregiudizievoli che potrebbe comportare la diffusione delle medesime

- **Interessati:** persone fisiche, identificate o identificabili, alle quali si riferiscono i Dati Personali
- **Misure di sicurezza tecniche organizzative:** Indicazione delle misure, specifiche per ciascun processo, che mitigano il rischio di trattamento improprio (es. eccedente rispetto agli obiettivi aziendali o effettuato da persona che non sono incaricate del trattamento) dei dati. A titolo puramente esemplificativo, alcune misure sono ad esempio il blocco delle porte USB, l'accesso vincolato a sistemi utilizzati esclusivamente da specifiche funzioni, procedure riguardanti il trattamento dei dati che prevedono specifiche modalità di catalogazione/archiviazione dei dati
- **Responsabili del Trattamento:** ai sensi dell'articolo 4 comma 8) per responsabile del trattamento si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento
- **Rete:** sistema di trasmissione dati che interconnette nodi indipendentemente dalla tecnologia utilizzata
- **Rete M4:** rete aziendale di M4 in cui sono disponibili i servizi applicativi di backoffice, le risorse di rete per la condivisione di documenti, i servizi di autenticazione di dominio M4, etc.. e in cui sono attestate le PdL M4
- **Registro dei trattamenti:** Registro delle attività di trattamento svolte sotto la responsabilità del Titolare del trattamento o per conto del Titolare da parte un soggetto terzo
- **Soggetti terzi:** Soggetti esterni all'organizzazione che effettuano il trattamento di dati personali in nome e per conto della Società. Per i soggetti terzi si richiede la denominazione sociale e la sede legale. Ai sensi dell'articolo 4 comma 9) si intende per 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 4.5.2016 L 119/33 Gazzetta ufficiale dell'Unione europea IT 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
- **Strumenti Aziendali:** Tutte le dotazioni hardware e software e le risorse informatiche aziendali dell'M4
- **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

- **Trasferimenti di dati personali verso paesi extra-UE:** Ai sensi dell'articolo 4 comma 23) si intende per trattamento transfrontaliero: a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro
- **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
- **Violazione dei dati personali ovvero Data Breach:** 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

6. Principi generali sulla protezione dei dati personali

M4 si impegna a trattare i dati personali secondo i principi che seguono in linea con la normativa vigente:

6.1. Accountability

Nel rispetto del principio di "accountability" il Titolare del Trattamento di M4 ha predisposto misure di sicurezza tecniche e organizzative sufficienti a garantire una protezione adeguata dei dati personali, sulla base del livello di rischio tollerabile.

6.2. Liceità, Correttezza, Trasparenza e Base giuridica del trattamento

Ogni trattamento di dati personali effettuato da M4 è lecito ossia basato su uno delle seguenti basi giuridiche:

- **Consenso dell'Interessato** qualora l'Interessato abbia espresso liberamente ed esplicitamente il consenso al trattamento dei propri dati personali per una o più specifiche finalità (a fronte di un'esauritiva informativa).
- **Adempimento contrattuale** qualora il trattamento sia necessario all'esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.
- **Obbligo di legge (art. 6, lettera c.)** – qualora il trattamento sia necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento (ai sensi delle leggi dell'UE o di uno Stato membro).
- **Compiti di interesse pubblico** qualora il trattamento sia 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.
- **Interesse legittimo** – qualora il trattamento dei dati personali degli interessati sia necessario per il perseguimento di un legittimo interesse del Titolare, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato.

6.3. Limitazione della finalità e Minimizzazione dei dati

M4 tratta i dati personali degli interessati solo per le finalità per le quali sono stati raccolti e solo in relazione a finalità determinate, esplicite e legittime quali esplicitate nelle comunicazioni all'Interessato. Inoltre, il trattamento e i dati trattati da M4 sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. M4 non raccoglie e tratta dati personali non strettamente necessari al perseguimento delle finalità identificate.

6.4. Esattezza

M4 corregge ed aggiorna periodicamente i dati personali degli interessati garantendone la correttezza e che siano poste in essere appropriate misure per correggere i dati inaccurati o incompleti (ad esempio permettendo agli interessati di aggiornare i loro dati quando necessario).

6.5. Limitazione della conservazione (data retention)

Per il principio di Data Retention, i dati personali raccolti devono essere conservati per il solo periodo di tempo necessario al perseguimento delle finalità per cui sono raccolti e trattati e successivamente cancellati o anonimizzati. M4 ha definito e reso note all'interno del documento la "Data Retention Policy" disponibile nella bacheca aziendale le tempistiche di ritenzione dei dati che sono state identificate per ogni nuovo trattamento o modifica di un trattamento esistente. I termini di Data Retention sono riportati nel Retention Schedule allegato alla presente Procedura come allegato A.

6.6. Integrità e riservatezza

In M4 i dati personali sono trattati in modo da garantire un'adeguata sicurezza dei dati stessi, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

M4 garantisce l'integrità e la riservatezza dei dati personali trasferiti esternamente attraverso:

- Gestione contrattuale e utilizzo di clausole di riservatezza;
- Gestione contrattuale e nomina del fornitore a Responsabile esterno del trattamento corredata da istruzioni di sicurezza impartite dal Titolare;
- Audit periodici presso il Responsabile esterno del trattamento al fine di monitorare il rispetto dei requisiti.

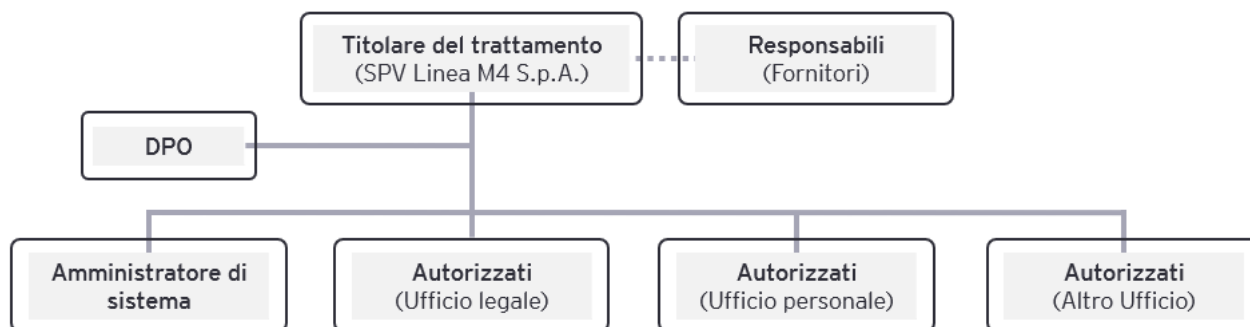
E' altresì garantita l'integrità e la riservatezza dei dati personali trattati internamente in qualità di Titolare o Responsabile esterno, attraverso l'applicazione delle procedure richiamate nel presente documento volte a proteggere dati trattati in forma cartacea e digitale e attraverso l'effettuazione di audit interni anche ad opera del DPO.

6.7. Privacy by design e by default

Il Titolare in M4 ha l'onere di definire la protezione dei dati personali fin dalla progettazione di un trattamento e per impostazione definita. Una nuova iniziativa, sin dalla sua progettazione, è ideata secondo un approccio "privacy oriented", volto a valutare se ciò che si sta progettando avrà un impatto sui dati personali e volto a identificare le misure di sicurezza organizzative e tecniche a protezione dei dati, da porre in essere prima di implementare il trattamento ("by design"). Durante la progettazione delle iniziative che comportano trattamenti di dati personali, è stato definito il trattamento in modo da coinvolgere i dati personali degli interessati nella misura e per il tempo necessari a raggiungere le finalità del trattamento ("by default").

7. Responsabilizzazione

M4 dispone di un organigramma privacy al fine di garantire la corretta gestione del sistema Privacy. In questo capitolo sono descritti i principali ruoli, compiti e responsabilità dei soggetti coinvolti nella gestione della Privacy.



7.1. Titolare del Trattamento

Il Titolare del Trattamento è il soggetto al quale competono le decisioni in ordine alle finalità e alle modalità del trattamento dei dati personali, ivi comprese le decisioni in merito all'adozione delle adeguate misure di sicurezza in modo da garantire un livello di sicurezza adeguato al rischio del trattamento.

7.2. Responsabile del Trattamento

Il Responsabile esterno del trattamento (di seguito Responsabile) è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del Trattamento dotato delle attitudini necessarie per mettere in atto misure tecniche e organizzative adeguate conformi ai requisiti del Regolamento, al fine di garantire la tutela dei diritti dell'Interessato e la tempestiva comunicazione di eventuali violazioni.

Il rapporto tra Titolare e Responsabile esterno è regolamentato con accordi contrattuali che M4 conclude di volta in volta con i differenti Responsabili Esterni ai fini di stabilire le misure tecniche ed organizzative di volta in volta necessarie per assicurare la tutela dell'Interessato.

7.3. Data Protection Officer

Il DPO è un esperto in materia privacy, con competenze giuridiche, informatiche, di risk management e di analisi dei processi.

M4 ha nominato un DPO i cui compiti, come individuati dalla legge sono quelli di fornire consulenza ed informare il Titolare sugli obblighi derivanti dalla legge relativi alla protezione dei dati personali, sorvegliare l'osservanza delle suddette previsioni di legge, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti ed alle relative attività di controllo, fornire – se richiesto – un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento, cooperare con l'Autorità privacy di Controllo e fungere da punto di contatto per l'Autorità medesima.

7.4. Amministratore di Sistema

M4 ha nominato un Amministratore di Sistema il quale, nei limiti descritti nella relativa lettera di nomina, ha lo scopo di garantire il regolare funzionamento dell'infrastruttura tecnologica aziendale e il corretto utilizzo della stessa da parte degli utenti interni ed esterni all'organizzazione.

L'Amministratore di Sistema in particolare è la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione e sistemi informativi con cui vengono effettuati trattamenti di dati personali. La figura dell'Amministratore di Sistema si configura come un utente con privilegi molto elevati tali da consentirgli di accedere e trattare una grande quantità di dati personali e di conseguenza aumentare il rischio intrinseco di perdita di confidenzialità, integrità e disponibilità degli stessi.

Per tale ragione l'Amministratore di Sistema, così come definito nell'atto di nomina, effettua esclusivamente le operazioni di trattamento strettamente necessarie alla corretta gestione e manutenzione dei Sistemi Informativi ("Operazioni"), nel rispetto dei principi di (i) liceità, correttezza e trasparenza, (ii) limitazione della finalità, (iii) minimizzazione dei dati, (iv) esattezza, (v) limitazione della conservazione, (vi) integrità e riservatezza.

8. Processi di Governance in materia di protezione dei dati personali

8.1. Informativa

M4 procede al trattamento di dati personali in modo deve essere corretto, ovvero non sono implementati trattamenti iniqui, ed è richiesta la trasparenza riguardo al trattamento dei dati personali.

Gli Interessati sono informati in modo aperto e trasparente in merito al trattamento dei propri dati personali prima che il trattamento venga implementato. In particolare l'Interessato viene informato tramite apposita Informativa, resa dal Titolare in forma chiara, concisa e facilmente comprensibile e accessibile, per metterlo nelle condizioni di conoscerne le intenzioni, le modalità del trattamento e per valutare se accettare o rifiutare il trattamento dei propri dati.

Ad ogni nuovo trattamento di dati personali, o modifica di un trattamento esistente, sono applicati i criteri di Privacy by Design: tra questi, viene sempre valutato, ove applicabile, la presenza di idonea informativa e di adeguata raccolta del consenso.

Agli Interessati a cui appartengono i dati, per via orale o per via scritta, viene di volta in volta fornita un'Informativa conforme a quanto previsto dagli art.13-14 del Regolamento Europeo.

8.2. Gestione Diritti degli Interessati

L'Interessato può esercitare nei confronti del Titolare:

- Il **diritto di accesso** dà all'Interessato il diritto accedere ai dati che lo riguardano e che sono oggetto di trattamento;
- Il **diritto di rettifica** consente all'Interessato di ottenere dal Titolare del trattamento la rettifica o l'integrazione dei dati personali non corretti;
- In base al **diritto alla cancellazione**, l'Interessato può richiedere al Titolare la cancellazione dei dati che lo riguardano;
- Il **diritto alla limitazione** si applica, per esempio, quando un Interessato richiede che i propri dati non siano più trattati per finalità di marketing. Il Titolare dovrà «contrassegnare» i dati personali e non utilizzarli più per finalità di marketing e utilizzarli per altre finalità;
- Per quanto riguarda la **portabilità dei dati**, l'Interessato ha diritto di ricevere dal Titolare copia dei suoi dati personali oggetto del trattamento e ha il diritto di richiedere al Titolare di trasmettere tali dati a un altro Titolare del trattamento;

- Il **diritto di opposizione**, infine, stabilisce che l'Interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano.

8.3. Gestione Terze parti e nomina dei responsabili esterni del trattamento

L'articolo 28 del Regolamento ha introdotto l'obbligo di nominare i responsabili esterni del trattamento. In adempimento di tale obbligo M4 procede a formalizzare le nomine di soggetti esterni che svolgono in favore del Titolare servizi che coinvolgono trattamenti di dati personali (si pensi, ad esempio, ai fornitori dei servizi di manutenzione dei sistemi IT, alle agenzie di teleselling, alle società di recupero credito, ecc.) mediante la nomina e Responsabili Esterni del trattamento dal Titolare, ovvero il Titolare disciplina tale rapporto attraverso un accordo contrattuale o altro atto giuridico.

8.4. Mappatura del Registro dei Trattamenti

M4 ha pertanto posto in essere il proprio registro dei trattamenti contenente i trattamenti effettuati in qualità di Titolare e Responsabile Esterno. Inoltre, in adempimento del disposto dell'articolo 30 del Regolamento Europeo M4 adempie all'obbligo, ivi previsto per i Titolari e per i Responsabili Esterni del trattamento, di mantenere aggiornato tale Registro dei Trattamenti, contenente l'elenco e la descrizione di tutti i trattamenti di dati personali effettuati sotto la propria responsabilità, al fine di consentire alle Autorità di controllo competenti di monitorare le attività di trattamento dei dati personali effettuate dal Titolare o dal Responsabile Esterno del trattamento. Il Registro è stato da ultimo aggiornato alla data di approvazione della presente procedura in data 10 Agosto 2025.

8.5. Gestione Data Breach

Al fine di definire e disciplinare all'interno di M4 le modalità operative per riconoscere registrare e notificare le violazioni di dati personali, è stato adottato a seguito di approvazione da parte del Consiglio di Amministrazione, il documento "Linee guida ed istruzione per la notifica di violazione di dati personali" consultabile nella bacheca aziendale

Con il termine "violazione di dati personali" (Personal Data Breach) si intende ogni evento che comporta accidentalmente o in modo illecito la perdita della Disponibilità (perdita della possibilità di accedere al dato, o la sua distruzione), Integrità (contenuto alterato) o Riservatezza (a causa di un'accidentale o non autorizzata diffusione o accesso al dato) del dato personale. Il documento recepisce l'obbligo previsto dal Regolamento Europeo a carico del Titolare del trattamento dei dati personali di notificare senza ingiustificato ritardo all'Autorità di Controllo e, in taluni casi, anche al soggetto Interessato, i casi di violazione dei dati personali con impatto sui diritti e le libertà dei soggetti interessati. Le Linee guida sopra citate, come previsto dal Regolamento Europeo, specificano altresì che a notifica deve essere inoltrata all'Autorità Garante competente senza ingiustificato ritardo ed entro 72 ore dal momento in cui il Titolare sia consapevole della violazione di dati personali.

8.6. Data Protection Impact Assessment

Al fine di adempiere al disposto dell'articolo 35 del Regolamento Europeo il quale recita che "quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali".

La valutazione di impatto o Data Protection Impact Assessment (DPIA) è una valutazione approfondita del rischio del trattamento ed è necessaria quando un trattamento presenta elevati rischio per le libertà degli Interessati al fine di permettere al Titolare di porre in essere misure di sicurezza adeguate sulla base del rischio intrinseco del

trattamento applicando così misure di sicurezza differenti a seconda del rischio rilevato.

M4 ha definito il documento “Procedura operativa DPIA” pubblicato nella bacheca aziendale al fine di permettere alle Funzioni Aziendali coinvolte nel trattamento di effettuare la valutazione e comprendere se il trattamento di dati personali è da considerare ad alto, medio o basso rischio privacy.

9. Le Misure di sicurezza ICT

Lo scopo della sicurezza informatica è assicurare l'integrità, la disponibilità e la confidenzialità dei dati e delle informazioni ed il rispetto delle normative vigenti in materia di privacy.

L'articolo 32 del Regolamento Europeo stabilisce, tra le altre, alcune delle misure di sicurezza e sottolinea la necessità di personalizzare le soluzioni di sicurezza da impostare, anche puntando all'efficienza organizzativa, tenuto conto dello stato dell'arte in cui opera il titolare, i costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento.

Al fine di assicurare un adeguato livello di sicurezza delle informazioni, M4 ha predisposto sia una serie di misure e strumenti tecnici sia un insieme di regole e norme comportamentali che devono essere seguite ed osservate da tutte le persone di M4 (dipendenti, consulenti, collaboratori, fornitori) che trattano informazioni elettroniche e cartacee menzionate, tra l'altro, nel documento “Regolamento per l'utilizzo degli strumenti informatici aziendali” pubblicato nella bacheca aziendale.

9.1. Disposizioni in merito alle modalità d'uso degli strumenti aziendali e verifiche

Un corretto utilizzo della strumentazione informatica permette un più efficiente svolgimento delle attività lavorative. **La dotazione informatica è lo strumento principale attraverso il quale sono gestiti i dati personali. Il Titolare del trattamento fornisce istruzioni alle persone che operano sotto la sua direzione per le attività di trattamento e, di conseguenza sui sistemi utilizzati per il trattamento.**

A questo scopo M4 ha definito il **“Regolamento per l'utilizzo degli strumenti informatici aziendali”** approvato dal Consiglio di Amministrazione in data 10/07/2023, disponibile nella bacheca aziendale. **Pertanto, si rinvia integralmente a tale Regolamento.**

Inoltre, si rende noto che, in ottemperanza ai doveri societari di salvaguardia dell'integrità delle infrastrutture informatiche e dei dati in esse contenuti, le verifiche possono riguardare: log di accesso e attività sui dispositivi aziendali (i dispositivi personali non sono utilizzabili in M4 se non previa autorizzazione), utilizzo della rete aziendale, accessi a file e cartelle condivise o cloud, nonché integrità e stato degli strumenti assegnati. Tali verifiche sono effettuate in forma aggregata per analisi di sicurezza o, individualmente, solo in presenza di fondati sospetti di violazioni dei regolamenti vigenti, di incidenti di sicurezza o di danni al patrimonio aziendale, nel pieno rispetto delle garanzie di legge.

I dati eventualmente raccolti durante le attività di controllo saranno trattati esclusivamente da personale autorizzato e conservati per il tempo strettamente necessario alle finalità perseguite. Il lavoratore può esercitare i diritti previsti dagli articoli 15-22 del GDPR rivolgendosi al Titolare o al DPO.

9.2. Principi generali sulla sicurezza delle informazioni

Il Titolare del Trattamento, come pure il Responsabile del Trattamento, è obbligato ad adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio del trattamento (con l'obiettivo di evitare distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato).

Il Regolamento per l'utilizzo degli strumenti informatici aziendali si integra con i principi generali di sicurezza delle informazioni per assicurare il controllo degli accessi. In particolare, per le logiche di assegnazione dei diritti di accesso:

- **Il principio del Privilegio Minimo:** i controlli di accesso devono essere assegnati sulla base delle esigenze aziendali e del "Least Privilege". Agli utenti devono essere concessi solo i diritti di accesso minimi ai sistemi, ai servizi, alle informazioni e alle risorse di cui hanno bisogno per svolgere le attività connesse al ruolo aziendale.
- **Il principio del Need To Know:** i controlli di accesso devono garantire la riservatezza delle informazioni, ciò implica che l'accesso deve essere concesso solo alle persone coinvolte direttamente nell'attività o nelle responsabilità per cui le informazioni sono rilevanti, riducendo così il rischio di divulgazione o accesso non autorizzato.
- **Segregation of Duties:** è un principio di controllo interno che prevede la separazione delle responsabilità chiave in un processo aziendale tra più persone in modo che nessuno abbia il controllo completo su un'intera attività o processo così da garantire la trasparenza, la responsabilità e la sicurezza delle operazioni aziendali.

10. Formazione e Consapevolezza

Come previsto dall'articolo 29 del GDPR, la normativa impone alle organizzazioni di istruire coloro che trattano i dati personali sotto la propria direzione e coordinamento. In particolare, il Regolamento attribuisce al Titolare il compito di diffondere la cultura sulla protezione dei dati personali all'interno dell'organizzazione attraverso attività di sensibilizzazione e formazione.

In alcune occasioni, la formazione in ambito privacy si estende anche ai consumatori e beneficiari finali del servizio, a garanzia di un corretto flusso informativo in caso di richieste da parte degli interessati.

Le istruzioni ai sensi dell'art. 29 del GDPR possono essere fornite in svariate modalità: tramite corsi specializzanti per le figure che si occupano appositamente di privacy e di sicurezza, tramite pillole di sensibilizzazione, vademecum, newsletter e tramite qualunque mezzo che sia utile a trasmettere una cultura della privacy in linea con le esigenze di business all'interno del luogo di lavoro.

Come richiesto dalla normativa M4 ha intrapreso un percorso di formazione che prevede incontri con i dipendenti e training calendarizzato al fine di sensibilizzare ed informare i dipendenti riguardo alle tematiche privacy.

11. Sanzioni

Per quanto concerne le violazioni al presente regolamento, si rimanda a quanto espressamente specificato nella procedura "Regolamento per l'utilizzo degli strumenti informatici aziendali", al punto 5.2.12 (Violazioni e sanzioni)

12. Modifiche e aggiornamenti

In caso di modifiche successive ritenute necessarie/opportune gli uffici emittenti provvederanno ad aggiornare il documento e riattivare in coordinamento con l'Ufficio Legale l'iter di approvazione da parte del Consiglio di Amministrazione. Gli uffici emittenti hanno altresì il compito di monitorare nel tempo l'adeguatezza ed effettiva applicazione del presente Regolamento.

13. Diffusione

La Segreteria Societaria è responsabile di archiviare in apposite cartelle di rete aziendali e diffondere internamente la procedura ed ogni sua successiva modifica/aggiornamento a seguito di approvazione da parte del Consiglio di Amministrazione.

14. Altri Riferimenti e Disposizioni Finali

- Policy di ritenzione dei dati personali
- Registro dei Trattamenti
- Procedura DPIA M4
- Linee guida e istruzioni per la notifica di violazione dei dati personali
- Comunicazione organizzativa – Persone autorizzate al trattamento dei dati personali ai sensi del Reg. UE n.679/2016 ovvero soggetti muniti di specifiche funzioni e compiti ex art. 2-quaterdecies del D.lgs n.196/2003
- Informativa dipendenti ai fini *privacy* ai sensi dell'art. 13 Reg. UE n. 679/2016
- Regolamento per l'utilizzo degli strumenti informatici aziendali
- Atto di Nomina ad Amministratore di Sistema
- Descrizione delle infrastrutture dei sistemi informativi di M4
- Statuto della Società SPV Linea M4 S.p.A.;
- Codice Etico e di Comportamento di M4 S.p.A.;
- Modello di Organizzazione Gestione e Controllo di M4 S.p.A. ai sensi del D.lgs. 231/2001
- Legge 300/1970 (Statuto dei Lavoratori)

ALLEGATO A – TERMINI DI DATA RETENTION

Verifica Protocollo di Legalità e Autorizzazioni alla Contrattualizzazione

Tipologia di Dati	Periodo di Conservazione	Riferimenti Normativi / Motivazione
Dati identificativi del fornitore, legale rappresentante e referenti	10 anni dalla cessazione del rapporto o dalla procedura	Esigenze probatorie, audit e responsabilità amministrativa
Documentazione antimafia (visure, comunicazioni prefettizie, dichiarazioni)	10 anni	Verifiche, audit, trasparenza e tracciabilità
Verbali, esiti dei controlli, autorizzazioni alla contrattualizzazione	10 anni dalla stipula del contratto o dalla chiusura della procedura	Prevenzione, difesa in giudizio, trasparenza amministrativa
Corrispondenze con organi pubblici (Prefettura, ANAC, MIT)	10 anni	Prova in caso di contenzioso o ispezione
Dati contenuti in white list, DURC, sistemi di controllo accessi	10 anni	Obblighi pubblicitici, tracciabilità, D.Lgs. 36/2023

Videosorveglianza in Tempo Reale (senza registrazione)

Tipologia di Dati	Periodo di Conservazione	Riferimenti Normativi / Motivazione

Sinistri Attivi e Passivi in Costruzione

Tipologia di Dati	Periodo di Conservazione	Riferimenti Normativi / Motivazione
Dati identificativi e di contatto del responsabile del sinistro	10 anni dalla definizione del caso	Prescrizione ordinaria responsabilità civile (art. 2946 c.c.)
Documentazione relativa al sinistro (foto, relazioni, testimonianze)	10 anni dalla chiusura del sinistro	Difesa in giudizio, accertamento tecnico e responsabilità
Dati relativi al recupero crediti (solleciti, decreti ingiuntivi)	10 anni dalla conclusione del procedimento	Prova in caso di contenzioso, obblighi fiscali
Documenti contabili connessi al danno o al recupero	10 anni	Conservazione contabile e fiscale (art. 2220 c.c.)
Dati trattati nell'ambito di eventuali contenziosi	Fino alla definizione definitiva della controversia	Difesa legale, responsabilità amministrativa
Dati identificativi e di contatto del danneggiato/testimoni	10 anni dalla definizione del caso	Prescrizione extracontrattuale (art. 2947 c.c.)

Documentazione tecnica e medico-legale relativa al sinistro	10 anni dalla chiusura del sinistro	Gestione responsabilità, contabile, assicurativa
Dati su gestione assicurativa e risarcimento	10 anni	Obblighi civilistici e assicurativi
Documentazione contabile relativa al risarcimento	10 anni	Obbligo di conservazione fiscale (art. 2220 c.c.)
Dati relativi a contenziosi legati al sinistro passivo	Fino alla definizione definitiva della controversia	Difesa in giudizio e responsabilità

Sicurezza dei Sistemi e Assistenza Tecnica IT

Tipologia di Dati	Periodo di Conservazione	Riferimenti Normativi / Motivazione
non presenti, si usa una corrispondenza e-mail per dare nota dell'intervento senza tenere alcuna traccia di dati personali		
non ce l'abbiamo		
Backup temporanei generati per assistenza Non necessari	Fino a 30 giorni	Principio di minimizzazione e storage limitation (art. 5.1.c- e GDPR)
Non necessari	12-24 mesi	Tracciabilità, qualità del servizio, audit IT
non necessari	Nessuna conservazione, salvo richiesta specifica e documentata	Devono essere eliminati subito dopo l'intervento
Come sopra, punto già trattato		
Log di sicurezza (firewall, antivirus, SIEM, alert)	12-24 mesi	Necessari per audit, data breach, gestione incidenti
Backup dei dati	Da 1 giorni a 12 mesi	Definito da necessità operative degli utenti
Documentazione su incidenti di sicurezza (es. data breach,	5anni	Prova per audit, responsabilità, notifiche

crash)		autorità
Non siamo soggetti		
Non siamo soggetti		

Gestione Ingressi Personale e Visitatori

Tipologia di Dati	Periodo di Conservazione	Riferimenti Normativi / Motivazione
Log di accesso tramite badge, tornello o registro elettronico (personale)	6–24 mesi	Provvedimento Garante 27/11/2008; art. 5 GDPR (minimizzazione)
Dati identificativi associati al badge (nome, ID, codice)	6–24 mesi	Tracciabilità accessi, coerenza con log
Dati biometrici (template impronta digitale)	Per tutta la durata del rapporto di lavoro, poi cancellazione immediata	Art. 9 GDPR; minimizzazione e sicurezza rafforzata
Dati relativi ad eventi anomali (accessi non autorizzati)	Fino alla definizione dell'evento o della controversia	Per fini probatori e di difesa legale
Log accesso visitatori (nome, data, orario, area)	6–12 mesi	Art. 5 GDPR; prassi comune e finalità di sicurezza
Registri cartacei o badge temporanei visitatori	6–12 mesi	Tracciabilità e controllo accessi
Foto o scansioni di documenti identificativi (se richiesti)	Fino alla verifica, max 24–72 ore	Limitazione della conservazione; finalità verifiche identità
Dati su accessi anomali o incidenti (visitatori)	Fino alla definizione dell'evento o controversia	Finalità difensive, audit e ricostruzione eventi

Gestione degli ingressi del personale dipendente (incluso accesso biometrico)

Tipologia di Dati	Periodo di Conservazione	Riferimenti Normativi / Motivazione
Log di accesso tramite badge, tornello o registro elettronico	sempre per tutta la durata del rapporto lavorativo	Provvedimento Garante 27/11/2008; principio di minimizzazione (art. 5 GDPR)
Dati identificativi del dipendente e associazione badge	sempre per tutta la durata del rapporto lavorativo	Necessario per la ricostruzione degli accessi e la tracciabilità

--	--	--

Gestione Eventi

Tipologia di Dati	Periodo di Conservazione	Riferimenti Normativi / Motivazione
Dati identificativi e di contatto dei partecipanti	12 mesi dalla conclusione dell'evento	Comunicazioni post-evento, gestione reclami, reportistica (art. 5 GDPR)
Materiale fotografico/video acquisito durante l'evento (previo consenso)	Fino a revoca del consenso o 2 anni	Marketing, comunicazione, archivio storico (artt. 6, 7 e 17 GDPR)
Dati organizzativi/logistici (es. preferenze alimentari, accessibilità)	Eliminazione immediata dopo l'evento	Minimizzazione e limitazione della conservazione (art. 5 GDPR)
Dati di fatturazione o rimborsi spese (se previsti)	10 anni	Obblighi civilistici e fiscali (art. 2220 c.c.)

Adempimenti D.Lgs. 231/2001

Tipologia di Dati	Periodo di Conservazione	Riferimenti Normativi / Motivazione
Flussi informativi verso l'Organismo di Vigilanza (OdV)	10 anni	Responsabilità organizzativa ex D.Lgs. 231/2001; art. 2220 c.c.
Documentazione di audit e controlli 231 (checklist, verbali, firme)	10 anni	Prova dell'efficacia del MOGC e per accountability (art. 6 D.Lgs. 231/2001)
Segnalazioni whistleblowing (anche anonime, se rilevanti)	5 anni dalla ricezione o dalla conclusione dell'istruttoria	Art. 14 D.Lgs. 24/2023 – tracciabilità e protezione del segnalante
Dati relativi a procedimenti disciplinari interni connessi alla 231	10 anni	Difesa in giudizio e responsabilità interna
Altri dati amministrativi e di supporto al Modello 231	10 anni	Conservazione amministrativa e controllo dell'efficacia del modello

Gestione Contenziosi (Dipendenti, Terzi, Societari)

Tipologia di Dati	Periodo di Conservazione	Riferimenti Normativi / Motivazione
Documentazione relativa ai contenziosi con dipendenti/ex-dipendenti (atti giudiziari, corrispondenza)	Fino a conclusione del procedimento, inclusi eventuali appelli	Necessario per la difesa in giudizio
Dati anagrafici e contrattuali dei soggetti coinvolti nel contenzioso	10 anni dalla conclusione del rapporto	Prescrizione civile ordinaria (art. 2946 c.c.), obblighi fiscali e probatori
Documentazione relativa ai	Fino a completa definizione	Difesa legale, principio di

contenziosi con fornitori, collaboratori, espropriati	del procedimento, inclusi eventuali appelli	limitazione della conservazione (art. 5.1.e GDPR)
Dati inerenti al rapporto contrattuale con le controparti (es. professionisti, fornitori)	10 anni dalla cessazione del rapporto	Prescrizione civilistica, obblighi fiscali e contabili
Documentazione su obblighi precedenti al contenzioso (appalti, responsabilità, pagamenti)	10 anni dalla conclusione del rapporto o adempimento	Obblighi contabili e fiscali (art. 2220 c.c.)
Atti giudiziari e documenti legali relativi a contenziosi societari	Fino a definizione completa, compreso eventuale giudicato	Difesa della società in giudizio
Documentazione societaria e amministrativa connessa al contenzioso (delibere, procure, contratti)	10 anni dalla definizione del contenzioso	Prova documentale, audit, adempimenti civilistici e fiscali

Gestione degli Adempimenti Societari

Tipologia di Dati	Periodo di Conservazione	Riferimenti Normativi / Motivazione
Verbal di assemblea, CdA, comitati, delibere	10 anni almeno; consigliata conservazione illimitata	Art. 2220 c.c.; esigenza permanente di tracciabilità decisionale
Libri sociali obbligatori (libro soci, libro CdA, libro sindaci)	Conservazione permanente	Obbligo civilistico ex artt. 2421, 2478 c.c.
Procure, deleghe, atti societari notarili	10 anni dalla revoca o cessazione degli effetti	Prova giuridica e difesa in giudizio
Comunicazioni a enti pubblici (es. CCIAA, Agenzia Entrate)	10 anni	Obblighi amministrativi e fiscali
Documenti di nomina/revoca di organi sociali	10 anni dalla cessazione dell'incarico	Obblighi di trasparenza, controlli e responsabilità degli organi

Attività Pubblicitarie, Promozionali, Sponsorizzazione, Marketing, Comunicazione e Informazione – Tabella Retention

Finalità del trattamento	Categorie di dati personali	Periodo di conservazione	Motivazione / Riferimento
Attività di marketing diretto e invio comunicazioni commerciali via email, SMS, telefono, posta o altri canali	Dati identificativi e di contatto (nome, cognome, email, numero di telefono), preferenze dichiarate	Fino a revoca del consenso o 24 mesi dal rilascio del consenso	Basato sul consenso (art. 6.1.a GDPR); limite di 24 mesi raccomandato dal Garante Privacy (prov. 23 gennaio 2020)
Profilazione per erogazione di servizi	Dati di utilizzo, comportamentali,	Fino a revoca del consenso o 12 mesi	Basato sul consenso (art. 6.1.a GDPR);

personalizzati e analisi delle preferenze, abitudini, comportamenti di consumo	navigazione, cronologia interazioni, preferenze espresse, dati aggregati	dal rilascio del consenso	limite di 12 mesi raccomandato dal Garante Privacy (prov. 23 gennaio 2020)
--	--	---------------------------	--

Gestione del processo di esproprio e della liquidazione dell'indennità agli espropriati – Tabella Retention

Finalità del trattamento	Categorie di dati personali	Periodo di conservazione	Motivazione / Riferimento
Gestione del procedimento di esproprio e della liquidazione dell'indennità agli espropriati	Dati identificativi, dati catastali, dati di contatto, estremi bancari, documentazione amministrativa e tecnica	10 anni dalla conclusione del procedimento di esproprio	Necessità di conservazione a fini civilistici e probatori (art. 2946 c.c. – prescrizione ordinaria decennale)

Gestione del Personale e Recruiting

Categoria di Dati Personali	Periodo di Conservazione	Riferimenti Normativi / Motivazione
Dati anagrafici e contrattuali (es. contratti, CV selezionati)	10 anni dalla cessazione del rapporto	Art. 2946 c.c., obblighi fiscali e probatori
Documentazione retributiva e contributiva (es. LUL, CUD, UNIAMENS)	10 anni	Art. 43 DPR 600/1973, art. 2220 c.c.
Cartelle sanitarie e di rischio (per esposizione a rischi particolari)	40 anni	Art. 25 D.Lgs. 81/2008
Dati su presenze, permessi, ferie, badge	5 anni dalla registrazione	Art. 2948 c.c.
Documentazione disciplinare	5 anni dalla cessazione del rapporto (10 anni in caso di contenzioso)	Prescrizione civile e difesa in giudizio
Email aziendali e contenuti account di lavoro	6 mesi dalla cessazione del rapporto	Prov. Garante 13/07/2016, accountability EDPB
CV ricevuti per specifiche vacancy concluse senza assunzione	Fino a 6 mesi dalla conclusione della selezione	Tempo tecnico per eventuali reclami o aggiornamenti
Candidature spontanee / banca talenti	12 mesi, prorogabili fino a 24 mesi con rinnovo consenso	Art. 5.1.e GDPR, principio di limitazione
Candidati intervistati ma non assunti	Fino a 24 mesi dall'ultimo colloquio	Interesse legittimo del titolare, in assenza di opposizione
Candidati assunti	Come da retention HR ordinaria (es. 10 anni)	Continuità documentale per rapporto di lavoro
Dati relativi a benefit aziendali (es. auto, PC, carte)	5 anni dalla restituzione del bene o cessazione del	Responsabilità su uso beni aziendali, interesse legittimo

aziendali)	rapporto	
Dati su fondi sanitari / welfare / previdenza integrativa	10 anni dalla cessazione del rapporto	Obblighi fiscali e previdenziali
Dati relativi a polizze assicurative aziendali (adesioni, variazioni, sinistri)	10 anni dalla cessazione della copertura o evento	Contenzioso e prescrizione civile
Documentazione relativa a infortuni sul lavoro	10 anni (40 anni in caso di patologie gravi o rischi specifici)	Art. 25 D.Lgs. 81/2008, responsabilità del datore di lavoro
Contatti con assicurazioni e broker	5 anni dalla chiusura del rapporto o attività	Gestione operativa e accountability

Gestione dei Collegamenti ai Social Network

Tipologia di Dati	Periodo di Conservazione	Riferimenti Normativi / Motivazione
Menzioni, citazioni, articoli social o su sito web aziendale	2 anni dalla pubblicazione o fino a richiesta di rimozione	Non esiste un periodo specifico nel GDPR: tuttavia, la retention va stabilita in modo ragionevole, documentato e proporzionato alla finalità, nel rispetto del principio di storage limitation (art. 5 GDPR)
Contenuti promozionali (foto/video con persone identificabili) pubblicati con consenso	Fino a revoca del consenso o richiesta di cancellazione	Art. 6.1.a e 7 GDPR – consenso revocabile in ogni momento

Gestione del Ciclo Passivo (Fornitori e Professionisti)

Tipologia di Dati	Periodo di Conservazione	Riferimenti Normativi / Motivazione
Contratti di fornitura e incarico	10 anni dalla cessazione del rapporto	Art. 2946 c.c., finalità probatorie e difesa in giudizio
Fatture passive, note di credito, documenti fiscali	10 anni	Art. 2220 c.c.; art. 43 DPR 600/1973 (obblighi fiscali)
Dati identificativi e anagrafici dei fornitori (es. IBAN, P.IVA, referenti)	10 anni dalla chiusura del rapporto	Coerenza con documentazione contrattuale e contabile
Documentazione relativa ad appalti e subappalti (es. DURC, verifiche antimafia)	10 anni	Obblighi normativi ex D.Lgs. 81/2008 e Codice Appalti
Email e comunicazioni operative	5 anni dalla cessazione del rapporto o conclusione attività	Interesse legittimo alla documentazione e accountability
Dati bancari e informazioni sui pagamenti	10 anni	Collegati a obblighi fiscali e contabili

Gestione Carte Prepagate e Carte di Credito Aziendali

Tipologia di Dati	Periodo di Conservazione	Riferimenti Normativi / Motivazione
Dati identificativi relativi a carte assegnate (nominativo, codice carta, limiti, PIN)	5 anni dalla restituzione o cessazione del rapporto	Interesse legittimo aziendale per tracciabilità e responsabilità
Rendicontazione delle spese effettuate (estratti conto, ricevute allegate, note spese)	10 anni	Obblighi fiscali e contabili (art. 2220 c.c., art. 43 DPR 600/1973)
Documentazione sulle autorizzazioni interne e policy di utilizzo	10 anni	Finalità di audit interno e difesa in giudizio
Dati relativi a contestazioni, blocchi, frodi o irregolarità	5 anni dalla chiusura della segnalazione o del procedimento	Responsabilità aziendale e supporto alla difesa in caso di abusi o anomalie
Documentazione delle note spese e spese di rappresentanza (scontrini, ricevute, report allegati)	10 anni	Obblighi fiscali e contabili (art. 2220 c.c. e art. 43 DPR 600/1973)
Dati fiscali e contabili relativi ai rimborsi (es. bonifici, approvazioni, quietanze)	10 anni	Coerenza con obblighi dichiarativi e revisione fiscale
Dati relativi a sanzioni/multe e contestazioni stradali su veicoli aziendali	5 anni dalla notifica o chiusura del procedimento	Interesse legittimo per responsabilità amministrativa e tracciabilità
Documentazione relativa all'assegnazione del veicolo aziendale	5 anni dalla restituzione del mezzo o cessazione del rapporto	Gestione responsabilità e uso beni aziendali

Accesso civico, accesso generalizzato e accesso agli atti

Tipologia di Dati	Periodo di Conservazione	Riferimenti Normativi / Motivazione
Dati identificativi e di contatto del richiedente (accesso civico/generalizzato)	5 anni dalla conclusione del procedimento	Trasparenza, tracciabilità, responsabilità amministrativa (D.Lgs. 33/2013, art. 5 GDPR)
Richiesta, esito, diniego o oscuramento	5 anni	Audit, prova decisionale, diritto di difesa
Dati relativi a eventuali contenziosi (ricorsi TAR, Garante)	Fino alla definizione del procedimento	Difesa in giudizio
Dati per eventuale fatturazione (FOIA)	10 anni	Obblighi fiscali e contabili (art. 2220 c.c.)
Dati identificativi del richiedente e del controinteressato (accesso atti)	5 anni dalla conclusione del procedimento	Trasparenza, accountability (Legge 241/1990, art. 5 GDPR)
Richiesta e provvedimento amministrativo (accoglimento, diniego)	5 anni	Ricostruzione del procedimento, motivazione decisioni

Documentazione istruttoria interna	5 anni	Audit interno e responsabilità amministrativa
Dati relativi a contenziosi amministrativi	Fino alla definizione del procedimento	Tutela giudiziaria e responsabilità

Sicurezza sul Lavoro e Gestione Infortuni

Tipologia di Dati	Periodo di Conservazione	Riferimenti Normativi / Motivazione
Giudizi di idoneità alla mansione specifica (senza diagnosi)	10 anni dalla cessazione del rapporto	Buona prassi per responsabilità del datore di lavoro; ricostruzione ex post
Cartelle sanitarie e di rischio	40 anni	Art. 25, co. 1 lett. b) D.Lgs. 81/2008
Registri di sorveglianza sanitaria / comunicazioni medico competente	10 anni	Obblighi documentali e audit sicurezza
Documentazione DUVRI e valutazione interferenze (appalti)	10 anni dalla cessazione del contratto	Art. 26 D.Lgs. 81/2008 – responsabilità solidale del committente
Documentazione sulla gestione lavoratori in somministrazione (idoneità, formazione, rischi)	10 anni	Obblighi sicurezza, tracciabilità contrattuale
Documentazione formazione e informazione sicurezza per appaltatori	10 anni	Obblighi artt. 36-37 D.Lgs. 81/2008
Dati su infortuni lavorativi o in itinere (es. report, certificati, dichiarazioni)	10 anni; 40 anni se connessi a patologie professionali	Art. 25 D.Lgs. 81/2008; responsabilità civile (art. 2946 c.c.)
Comunicazioni a INAIL / assicurazioni / Autorità competenti	10 anni	Obblighi assicurativi e contabili; difesa legale
Documentazione interna su dinamica dell'infortunio, testimoni, responsabilità	10 anni	Supporto contenzioso e audit interni
Documentazione sanitaria inviata dal lavoratore (fuori da cartella medica)	10 anni	Art. 9.2.b GDPR – obblighi in materia di diritto del lavoro
Verbal di audit interni su incidenti/infortuni	10 anni	Art. 30 D.Lgs. 81/2008 – miglioramento continuo sicurezza