



Privacy Policy di Gruppo 2023

Versione:
Maggio 2023





Questa Policy assicura regole e linee guida per la gestione del trattamento dei dati personali, in accordo con quanto previsto dal Regolamento europeo (UE) n. 2016/679 (GDPR) e delle normative locali che disciplinano la materia, da parte delle Società del Gruppo Lavazza soggette all'applicazione del GDPR.

Versione	Data	Descrizione	
V. 3	Maggio 2023	<i>Prima versione: Novembre 2018 Seconda versione: Ottobre 2020 Terza versione: Maggio 2023</i>	
FUNZIONE COMPETENTE:		<i>Policies, Guidelines and Procedures</i>	
OWNER DELL'ATTIVITÀ:		<i>DPO</i>	
VAGLIATO DA:		<i>Legal, Corporate Affairs & Compliance</i>	
		<i>HR</i>	
		<i>IT</i>	
		<i>Internal Auditing</i>	
APPROVATO DA:		<i>CEO</i>	

CONTENUTO

1.	INTRODUZIONE	4
2.	PRINCIPI GENERALI	9
2.1	PREMESSA	9
2.2	DEFINIZIONE DI DATO PERSONALE	10
3.	MODELLO ORGANIZZATIVO PRIVACY (M.O.P.)	11
3.1	PREMESSA	11
3.2	RUOLI NELL'AMBITO DEL GRUPPO LAVAZZA	11
3.3	TITOLARE DEL TRATTAMENTO	12
3.4	DELEGATO DEL TITOLARE	12
3.5	RESPONSABILE DEL TRATTAMENTO (SOCIETÀ DEL GRUPPO E TERZE PARTI)	13
3.5.1	Società del Gruppo	13
3.5.2	Terze parti	13
3.6	DATA PROTECTION OFFICER	14
3.7	COMITATO PRIVACY	15
3.8	FOCAL POINT PRIVACY DELLE SOCIETÀ DEL GRUPPO LAVAZZA	15
3.9	REFERENTI INTERNI ALLE SOCIETÀ DEL GRUPPO LAVAZZA	15
3.10	AUTORIZZATI AL TRATTAMENTO	16
3.10.1	Autorizzati al trattamento di videosorveglianza	17
4.	REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO	17
5.	MODELLO DI GESTIONE	17
5.1	RACCOLTA	18
5.1.1	Finalità	18
5.1.2	Base giuridica	18
5.1.2.1	Il consenso	18
5.1.2.2	Esecuzione di un contratto	20
5.1.2.3	Adempimento di un obbligo di legge	20
5.1.2.4	Legittimo interesse	20
5.1.3	L'informativa privacy	21
5.2	TRATTAMENTO – PRINCIPI GENERALI	21
5.2.1	Trattamento effettuato da Terze Parti	22
5.2.2	Trasferimenti transfrontalieri di dati personali– Flussi infragruppo	22
5.2.3	Cookies e tecnologie similari	23
5.2.4	Sicurezza	24
5.3	TRATTAMENTI SPECIFICI - CESSAZIONE DEL TRATTAMENTO - CANCELLAZIONE E DISTRUZIONE	24
6.	DIRITTI DELL'INTERESSATO E RISCONTRO	25
6.1	DIRITTO DI ACCESSO	25
6.2	DIRITTO DI RETTIFICA	25
6.3	DIRITTO ALLA CANCELLAZIONE	25
6.4	DIRITTO DI LIMITAZIONE AL TRATTAMENTO	26
6.5	DIRITTO ALLA PORTABILITÀ DEI DATI	26
6.6	DIRITTO DI OPPOSIZIONE	26
6.7	RISPOSTA AL RICHIEDENTE E TERMINI PREVISTI	27
7.	ISTRUZIONI OPERATIVE	27
8.	PRIVACY BY DESIGN & BY DEFAULT	27
9.	VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)	28
10.	VALUTAZIONE D'IMPATTO SUL TRASFERIMENTO DEI DATI (TIA)	29



11. NOTIFICA IN CASO DI VIOLAZIONE DEI DATI PERSONALI	29
12. ISPEZIONI DELL'AUTORITÀ DI CONTROLLO	30
12.1 REGOLE COMPORTAMENTALI IN CASO DI ATTIVITÀ ISPETTIVE	31
13. FORMAZIONE	31
14. AUDIT	32
15. SANZIONI.....	32

1. Introduzione

Ambito di applicazione e scopo La presente Policy si applica alla LUIGI LAVAZZA S.p.A. (anche “Capogruppo”) e/o alle sue Consociate, italiane ed estere (di seguito singolarmente “Società” o “Consociata” e collettivamente “**Gruppo LAVAZZA**”), soggette all’applicazione del GDPR, nelle attività di trattamento di dati personali (così come definiti nel paragrafo 2.2.) nel corso dello svolgimento dell’attività di business.

Lo scopo del documento è quello di disciplinare le attività di trattamento di dati personali all’interno del Gruppo LAVAZZA, al fine di garantire la piena conformità alle disposizioni dettate dal Regolamento Europeo n. 2016/679 (GDPR)

Responsabilità **Tutti i Managers del Gruppo sono responsabili di garantire il rispetto della presente Policy. In particolare, tutti i soggetti coinvolti nel trattamento di dati personali devono contribuire alla protezione dei dati personali dando applicazione alla presente Policy ed ai “Privacy Principles” di seguito indicati.**

La presente Policy potrà venire implementata e integrata, ove necessario, a seguito di indicazioni da parte della Funzione Corporate Affairs & Compliance della Capogruppo LUIGI LAVAZZA S.p.A. e da parte del DPO di Gruppo.


PRINCIPI PRIVACY

Trattamento e finalità Il Gruppo LAVAZZA tratta i dati personali **in modo lecito, corretto e trasparente**, per il raggiungimento delle **finalità di business** che siano **determinate, esplicite e legittime**, e adotta misure ragionevoli per garantire che i dati personali siano **esatti** e, se necessario, **aggiornati**.

Terze parti Le Terze Parti (fornitori, business partner, consulenti) che entrano a qualsiasi titolo in rapporto d’affari con le Società del Gruppo LAVAZZA e, in virtù di ciò, effettuano operazioni di trattamento di dati personali per conto delle stesse, sono designate **Responsabili del trattamento** e sono contrattualmente vincolate al rispetto delle misure per la sicurezza e la riservatezza dei dati, nonché ad astenersi da qualunque utilizzo o divulgazione che non sia autorizzata dal Gruppo LAVAZZA.
Il Gruppo LAVAZZA attribuisce particolare importanza alla protezione della **riservatezza** dei dati personali, sollecitando il contributo di tutti i collaboratori, interni ed esterni, nel raggiungimento di tale obiettivo.

Comunicazione dei dati personali I dati personali conferiti possono essere **comunicati** a soggetti terzi per adempiere ad obblighi di legge, in esecuzione di ordini provenienti da pubbliche autorità ovvero per fare valere o difendere un diritto in sede giudiziaria, nonché nell’ambito delle Società facenti parte del Gruppo LAVAZZA per necessità di business e per fini amministrativi interni, compreso il trattamento dati personali di clienti e dipendenti.
I dati personali possono essere comunicati a soggetti terzi, in qualità di autonomi Titolari del trattamento o di Responsabili del trattamento, con il **consenso** degli Interessati, se richiesto per legge, e comunque previa adeguata informativa volta a specificare le finalità del trattamento. I dati personali non sono **diffusi**.

Conservazione I dati personali sono conservati solo per il **tempo necessario** a raggiungere le finalità per le quali sono stati raccolti o in conformità ai termini previsti per legge o necessari per far valere un diritto in sede giudiziaria. I dati personali sono conservati in conformità alla Retention Policy di Gruppo, resa disponibile ai dipendenti nella intranet

**Rapporti di lavoro**

aziendale nella sezione Our Privacy - Policy & Procedure, salvo vi siano esigenze di conservazione differenti dettate da normative locali.

Con riferimento ai dati che le Società trattano nello svolgimento dei **rapporti di lavoro**, il Gruppo LAVAZZA utilizza i dati personali solo per il raggiungimento delle finalità connesse (quali, ad es., esecuzione del rapporto di lavoro; payroll, benefits, adempimenti fiscali, assistenziali e previdenziali, igiene e sicurezza sul lavoro; attività formative e di sviluppo della carriera, valutazione delle performance; utilizzo di dati personali, incluse immagini fotografiche e video, per scopi istituzionali).

Attività commerciali e di marketing

Nel rispetto dei principi di **liceità, correttezza e trasparenza**, e con il previo **consenso** degli Interessati se richiesto per legge, il Gruppo LAVAZZA può trattare dati personali per il raggiungimento di finalità commerciali e di marketing (quali, ad es., invio di materiale pubblicitario e altre iniziative promozionali e di marketing; attività di vendita diretta; analisi su abitudini e scelte di consumo ed elaborazioni statistiche).

Sicurezza

Il Gruppo LAVAZZA adotta **tecnologie sicure e ragionevoli precauzioni per proteggere i dati personali** contro l'indebita divulgazione, alterazione o uso improprio. Le protezioni attivate si propongono, in particolare, di ridurre al minimo i rischi di distruzione e di perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Nell'ambito del Gruppo vengono condotte attività periodiche di **analisi dei rischi** per verificare l'aderenza agli standard di sicurezza definiti ed eventualmente adottare nuove misure di sicurezza a seguito di cambiamenti organizzativi ed innovazioni tecnologiche o cambiamenti nella tipologia dei dati raccolti. Le misure di sicurezza sono **costantemente controllate e periodicamente verificate**.

Self - Assessment

Il Gruppo LAVAZZA effettua una **periodica autovalutazione** al fine di verificare che la presente Policy venga applicata in tutto il Gruppo e che tutte le persone all'interno del Gruppo si conformino ai presenti *Principles*.

Compliance

Nella definizione dei *Privacy Principles*, il Gruppo LAVAZZA si conforma al Regolamento europeo n. 679/2016 e, in generale, alle leggi ed ai regolamenti applicabili che tutelano la riservatezza dei dati personali nelle giurisdizioni in cui LUIGI LAVAZZA S.p.A. o le sue Società controllate operano. Specifiche giurisdizioni potrebbero richiedere che il Gruppo LAVAZZA integri la presente Policy per conformarsi alle leggi locali.

Contatto

Per qualsiasi domanda e/o dubbio riguardante l'applicazione della presente Policy, contattare il **DPO del Gruppo LAVAZZA** (privacyDPO@lavazza.com) o la **Funzione Corporate Affairs & Compliance** della Capogruppo.

Glossario

Al fine di agevolare la comprensione del presente documento, si riporta di seguito l'elenco di alcune parole chiave e relative definizioni:

- **Amministratore di Sistema:** persona fisica cui è demandata la gestione e/o la manutenzione di un sistema informatico e di elaborazione dati o di sue componenti sia *hardware* che *software*, come definiti dal Provvedimento Generale del Garante Privacy italiano del 27 Novembre 2008 e s.m.i.;
- **Autorità di controllo (o Autorità):** l'Autorità di cui all'articolo 51 del Regolamento Europeo in materia di Protezione dei Dati Personali ovvero una o più Autorità pubbliche indipendenti incaricate da uno Stato Membro di sorvegliare l'applicazione del Regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali. In Italia l'Autorità di controllo indipendente è il Garante per la protezione dei dati personali (cd. "Garante Privacy");
- **Autorizzato al trattamento:** persona fisica autorizzata a compiere materialmente le operazioni di trattamento su dati personali per conto del Titolare. E' autorizzato al trattamento tutto il personale dipendente che, in virtù delle mansioni svolte, si trovi a trattare dati personali.
- **Clausole Contrattuali Standard:** strumento di garanzia predisposto dalla Commissione Europea al fine di regolare e legittimare il trasferimento di dati personali al di fuori dello Spazio Economico Europeo.
- **Comitato Privacy:** gruppo di coordinamento per l'applicazione della normativa privacy istituito in seno alla Capogruppo e composto da rappresentanti delle funzioni aziendali HQ competenti in materia (HR, Internal Audit, Affari Legali e Societari, ICT, Digital Marketing, Marketing Italia e altre di volta in volta individuate);
- **Comunicazione:** il dare conoscenza dei dati personali a uno o più soggetti diversi dall'interessato, dal rappresentante del Titolare o del Responsabile non stabiliti nel territorio dell'Unione europea, dalle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile o espressamente designate, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
- **Consociata:** tutte le Società direttamente o indirettamente controllate da Luigi LAVAZZA S.p.A.
- **Data Processing Agreement ("DPA"):** accordo per il trattamento dei dati personali sottoscritto fra un Titolare ed un Responsabile del trattamento e volto a disciplinare dati, finalità e modalità del trattamento nonché le gli obblighi e le responsabilità delle parti;
- **Data Protection Impact Assessment ("DPIA"):** valutazione dei rischi connessi al trattamento dei dati personali e dell'impatto che il verificarsi dei rischi individuati può comportare sui diritti e le libertà dei soggetti interessati dai trattamenti;
- **Data Protection Officer o "Responsabile della protezione dei dati" (o "DPO"):** soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Coopera con l'Autorità e costituisce il

punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali;

- **Dati identificativi:** i dati identificativi sono i dati attraverso i quali è possibile ottenere l'identificazione diretta dell'interessato. A titolo esemplificativo i codici identificativi, sia quelli ricavati da dati anagrafici (e.g. codice fiscale) sia i codici univoci attribuiti a una persona in base a criteri predefiniti (e.g. codici cliente), sono dati identificativi;
- **Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»), anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso 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;
- **Dato sensibile/particolare:** i Dati Personali idonei a rivelare 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;
- **Delegato del Titolare del trattamento:** persona fisica designata dal Titolare del trattamento allo svolgimento delle attività utili a garantire il costante e puntuale rispetto delle normative vigenti in materia di trattamento di dati personali, nonché a rappresentarlo nei rapporti con i soggetti interessati e le Autorità e in tutti gli atti e i contratti di nomina di Terze Parti;
- **Diffusione:** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- **Focal Point Privacy ("FPP"):** persona fisica, designata presso ogni Consociata, preposta come punto di contatto fra la Società stessa ed il DPO di Gruppo al fine di facilitare la gestione di tutte le tematiche e specificità locali inerenti il trattamento dei dati personali;
- **General Data Protection Regulation ("GDPR"):** il "*General Data Protection Regulation*", ossia il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, che stabilisce la disciplina europea di regolamentazione in ambito di protezione dei dati personali;
- **Gruppo LAVAZZA:** Luigi LAVAZZA S.p.A. e tutte le sue Consociate;
- **Headquarters ("HQ"):** sede legale della Luigi LAVAZZA S.p.A.
- **Interessato:** la persona fisica identificata o identificabile, direttamente o indirettamente, da un dato personale e comunque cui il dato trattato si riferisce;
- **Legittimate Interest Assesment ("LIA"):** bilanciamento fra gli interessi del Titolare che effettua un trattamento di dati personali sulla base del suo legittimo interesse e i diritti e le libertà degli interessati cui si riferiscono i dati personali trattati;
- **Luigi LAVAZZA S.p.A. (o Capogruppo):** la società capogruppo con sede legale in Via Bologna n. 32 - Torino (Italy); la sede legale è anche definita come Headquarters ("HQ");
- **Modello organizzativo privacy ("M.O.P."):** si intende un insieme di regole, procedure misure organizzative e tecniche adottate per garantire la conformità alle norme sulla protezione dei dati personali e sulla privacy.

- **Referente Interno:** persona fisica preposta a supportare il Titolare del trattamento nella corretta gestione e verifica della conformità dei trattamenti dei Dati Personali posti in essere all'interno della Direzione/Funzione di appartenenza;
- **Responsabile del Trattamento:** il soggetto (persona fisica o giuridica) a cui viene conferita la nomina a Responsabile in relazione ai trattamenti di dati personali compiuti per conto del Titolare, per effetto di un atto formale di nomina che definisce l'ambito di responsabilità assegnate;
- **Sub-Responsabile del Trattamento:** il soggetto (persona fisica o giuridica) che effettua le attività di trattamento affidategli dal Responsabile del trattamento;
- **Titolare del trattamento:** la persona fisica o giuridica che determina le finalità e i mezzi del trattamento di dati personali. Il titolare ha inoltre il compito di assicurare l'implementazione delle misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio;
- **Transfer Impact Assesment ("TIA"):** valutazione di impatto sul trasferimento dei dati personali al di fuori dell'UE e dello SEE e per i quali non sussistano le garanzie adeguate al trasferimento di cui al capo V° del GDPR.
- **Trasferimenti di dati personali:** qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo sito al di fuori dell'UE/SEE per il quale non sia stata emanata una decisione di adeguatezza, compresi trasferimenti successivi di dati personali da un paese terzo verso un altro paese terzo;
- **Trattamento:** qualunque operazione o complesso di operazioni, effettuati senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati, anche se non registrati in una banca di dati;
- **Violazione dei dati personali ("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.

2. Principi generali

2.1 Premessa

Il Regolamento Europeo n. 2016/679¹, meglio noto con la sigla GDPR (*“General Data Protection Regulation”*), è un regolamento dell'Unione europea in materia di **protezione delle persone fisiche con riguardo al trattamento dei dati personali**, volto a disciplinare in modo uniforme i diritti dei cittadini europei in materia di privacy.

Tali regole sono state concepite per **rafforzare la fiducia degli interessati**, rendendoli maggiormente edotti sul come vengono utilizzate le informazioni personali che li riguardano e liberi di decidere consapevolmente se acconsentire o meno ad un loro utilizzo².

Ciò comporta un significativo impatto sui dati che normalmente vengono dall'azienda raccolti e gestiti nell'ambito delle normali attività commerciali, di marketing, operative e in generale di business, in conseguenza dell'**innalzamento del livello di protezione dei dati personali** - relativi a clienti e consumatori, oltre che al personale dipendente e ai collaboratori - operato dal Regolamento.

Nell'ambito dello svolgimento della propria attività imprenditoriale, il Gruppo LAVAZZA raccoglie una quantità significativa di dati e di informazioni riservate, che si impegna a trattare in ottemperanza a tutte le leggi in materia di privacy e riservatezza vigenti nelle giurisdizioni in cui opera.

In particolare, nei principi espressi dal **Codice Etico del Gruppo LAVAZZA** è dichiarato quanto segue: *“Ci impegniamo per proteggere qualunque informazione sensibile, riservata e proprietaria che riguardi il Gruppo. La riservatezza è essenziale per garantire fiducia e autenticità, sia all'interno del Gruppo, sia nei rapporti con i partner e i consumatori”*.

Lo stesso impegno di riservatezza nell'utilizzo, nell'elaborazione e nella custodia dei dati, deve essere assunto e garantito da tutto il personale dipendente e non che, nell'esercizio delle proprie attività, effettua il trattamento di dati personali per conto del Gruppo LAVAZZA.

I dipendenti e i collaboratori del Gruppo LAVAZZA, a tutti i livelli, sono pertanto tenuti a riconoscere se stanno raccogliendo, utilizzando, elaborando, conservando o condividendo dati personali oggetto di tutela. Devono essere, quindi, edotti e consapevoli dei **principi cardine che governano il trattamento dei dati personali**, ovvero che i dati:

- devono essere trattati in modo **lecito, corretto e trasparente** nei confronti dell'interessato, in conformità alle specifiche finalità descritte in modo chiaro e comprensibile nell'informativa sulla privacy e sulla base dei presupposti di liceità che ne giustificano il trattamento (tra cui il consenso esplicito al trattamento, laddove necessario);
- devono essere raccolti per **finalità determinate, esplicite e legittime** e successivamente trattati con modalità non incompatibili con tali finalità (*“Principio di limitazione della finalità”*);

¹ Successivamente all'entrata in vigore del GDPR, in data 10 agosto 2018 è stato emanato, a scopo di coordinamento con la previgente normativa italiana, il D. Lgs. n. 101/2018 recante *“Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679”*.

² Il GDPR si prefigge lo scopo di fornire un livello di protezione più elevato riguardo al trattamento di dati personali effettuato (i) sia dai **Titolari del trattamento operanti nel territorio dell'UE/SEE, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione** (ii) che di quelli **stabiliti al di fuori dell'UE/SEE, ma che gestiscono dati di consumatori europei offrendo prodotti e servizi nel territorio UE (indipendentemente dal fatto che vi sia un pagamento correlato)**.

- devono essere **adeguati, pertinenti e limitati a quanto necessario** rispetto alle finalità per le quali sono trattati (“*Principio di minimizzazione*”);
- devono essere **esatti** e, se necessario, **aggiornati**;
- devono essere conservati in una forma che consenta l’identificazione degli interessati **per un arco di tempo non superiore al conseguimento delle finalità** per le quali sono trattati (“*Principio di limitazione della conservazione*”);
- devono essere trattati in modo da garantire un’**adeguata sicurezza** dei dati personali, compresa la protezione - mediante misure tecniche e organizzative adeguate - da trattamenti non autorizzati o illeciti e dalla perdita, distruzione, modifica, rivelazione o accesso non autorizzati che potrebbero cagionare un danno.

Il rispetto di tali principi è responsabilità del **Titolare del trattamento**, supportato dal Data Protection Officer- DPO, e comporta una **valutazione**, una **gestione** e un **monitoraggio continuo del rischio**.

Ciascun Referente Privacy (Referente Interno) delle Società del Gruppo, così come individuato al successivo paragrafo 3.9, ha il compito di far rispettare la presente Policy nella propria area funzionale di responsabilità.

Tutti i dipendenti/collaboratori del Gruppo LAVAZZA sono responsabili del rispetto dei principi e delle regole definite nel presente documento.

L’osservanza delle disposizioni della presente Policy deve considerarsi parte essenziale delle obbligazioni contrattuali dei dipendenti/collaboratori.

Le violazioni della presente Policy possono condurre ad un’**azione disciplinare** inclusi – nei casi più gravi – il licenziamento, nel rispetto delle leggi vigenti e dei contratti di lavoro nazionali, o la cessazione del rapporto di collaborazione (per i soggetti terzi).

Il rispetto delle disposizioni di legge in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, oltre a rappresentare un approccio in linea con i principi recepiti nel Codice Etico di Gruppo e nei documenti correlati costituisce, altresì, un’**importante occasione per razionalizzare, classificare e ordinare i dati personali custoditi in azienda secondo criteri di necessità e di sicurezza aggiornati, limitando la duplicazione di dati in eccesso ed evitando i rischi associati ai trattamenti degli stessi.**

2.2 Definizione di dato personale³

Per dato personale si intende **qualsiasi informazione riguardante una persona fisica identificata o identificabile (“*Interessato*”), direttamente o indirettamente**, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online⁴ o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale⁵.

³ Il GDPR non si applica ai trattamenti di dati personali effettuati per l’esercizio di **attività a carattere esclusivamente personale o domestico**.

⁴ Gli identificativi online prodotti da dispositivi, dalle applicazioni, dagli strumenti (quali indirizzi IP, cookies, tag di identificazione, ecc.) possono lasciare tracce che, se combinate con identificativi univoci e altre informazioni ricevute dal server, possono identificare le persone fisiche. E’ compresa anche l’identificazione digitale dell’interessato, mediante meccanismo di autenticazione (quali le stesse credenziali utilizzate dall’interessato per l’accesso – *log in* – al servizio on line offerto dal Titolare del trattamento).

⁵ Il GDPR non si applica al trattamento di **informazioni anonime**, cioè (*i*) ad informazioni che non si riferiscono ad una persona fisica identificata o identificabile (*ii*) a dati personali resi sufficientemente anonimi da impedire o da non consentire più l’identificazione dell’Interessato. Il Regolamento non si applica, pertanto, al trattamento di informazioni anonime per finalità statistiche o di ricerca.

3. Modello organizzativo privacy (M.O.P.)

3.1 Premessa

Il presente paragrafo illustra i **ruoli**, definiti e coinvolti attivamente nella gestione del **Modello Organizzativo Privacy (M.O.P.)** all'interno del Gruppo LAVAZZA, e le **responsabilità** di applicazione del Modello sulle diverse strutture organizzative.

Le principali figure coinvolte nel modello di gestione per il trattamento dei dati personali sono:

- **Titolare del Trattamento**
- **Delegato del Titolare**
- **Responsabile del Trattamento** (Società del Gruppo e Terze Parti) ed eventuali Sub-Responsabili
- **Data Protection Officer**, locale e di Gruppo
- **Comitato Privacy**
- **Focal Point Privacy** delle Società del Gruppo
- **Referenti Interni** delle Società del Gruppo (di primo e secondo livello)
- **Autorizzati al trattamento**

3.2 Ruoli nell'ambito del Gruppo LAVAZZA

Tenuto conto dell'attività di *self-assessment* di Gruppo svolta sulla tipologia dei dati personali trattati, sui trattamenti infragruppo, sui processi organizzativi e sui presidi tecnologici, si è ritenuto che - **in via generale e salvo eccezioni - lo Stabilimento principale⁶, ove sono fornite le linee guida di Gruppo che riguardano i trattamenti di dati personali, corrisponde alla sede legale (HQ) della Capogruppo LUIGI LAVAZZA S.p.A., società individuata quale "capofila"⁷ per le tematiche di Data Protection.**

Presso la sede legale sono, infatti, effettivamente declinati e condivisi i principi e le regole da seguire, quando vengono trattati dati personali, nell'ambito del Gruppo ed indipendentemente dal fatto che i dati siano trattati presso quella sede⁸.

Benché gli indirizzi generali sul trattamento dei dati personali siano forniti dalla Capogruppo, a livello locale sono stati definiti i ruoli e le responsabilità di ciascuna Società in relazione al trattamento dei dati personali effettuato all'interno di ciascuna organizzazione.

In particolare, le Società del Gruppo possono trattare i dati personali in qualità di Titolari del trattamento ovvero di Responsabili del trattamento sulla base di appositi accordi per il trattamento dei dati personali (c.d. "**Framework Agreement**") volti a disciplinare – nell'ambito dei **rapporti infragruppo** - la natura, la finalità, la durata del trattamento, il tipo di dati personali, le categorie di interessati, gli obblighi e i diritti delle parti.

Luigi Lavazza S.p.A., in qualità di Società capofila, individua tra i primi riporti dell'Amministratore Delegato i **Referenti Interni di primo livello** incaricati di individuare e nominare, nell'ambito della propria funzione e secondo un processo a cascata, i "**Referenti Interni**" di **secondo livello**.

⁶ Ai sensi dell'art. 4, punto 16, GDPR e delle Linee Guida per l'individuazione dell'autorità di controllo capofila adottate il 5/4/2017 dal Gruppo di Lavoro art. 29

⁷ In senso conforme, l'art. 2.1.2. delle Linee Guida per l'individuazione dell'autorità di controllo capofila adottate il 5/4/2017 dal Gruppo di Lavoro art. 29 sancisce che "*qualora un trattamento sia svolto da un gruppo imprenditoriale la cui sede centrale è situata nell'UE, si presume che lo stabilimento dell'impresa controllante sia il centro decisionale con riguardo al trattamento di dati personali e, quindi, rappresenti lo stabilimento principale del gruppo*".

⁸ In senso conforme, cfr. *Considerando* 36 al GDPR

Per quanto concerne le altre Società del Gruppo, ogni soggetto responsabile di Consociata/e (“General Manager”/“Regional Director”) individua i **“Referenti Interni” di primo livello presso la Consociata**.

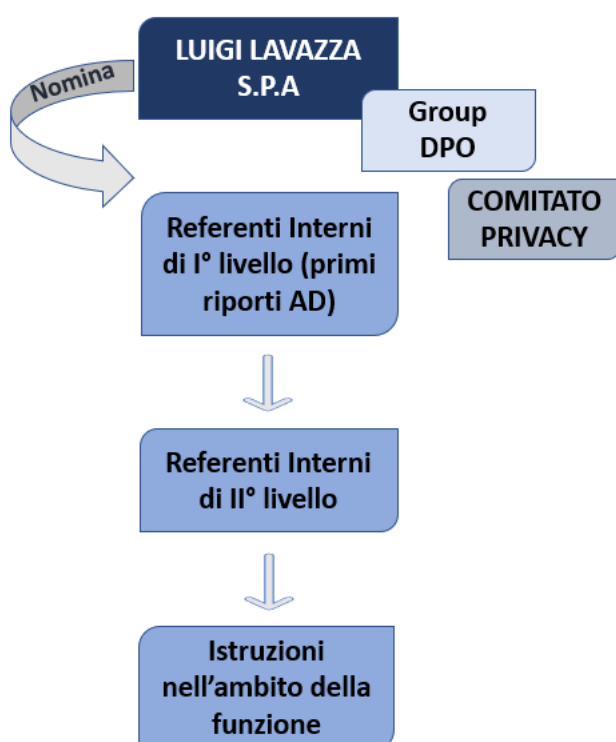
3.3 Titolare del Trattamento

Il Titolare è la persona fisica o giuridica che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali. Sulla base di tale definizione, sono state individuate le Società del Gruppo che agiscono in qualità di Titolari del trattamento.

La titolarità può essere riferita a tutti i dati personali trattati dalla Consociata (dati dei dipendenti/collaboratori, dati di clienti e di consumatori) ovvero ad una parte di essi (solo dati dei dipendenti/collaboratori o solo dati di clienti e di consumatori).

In particolare, per i dati personali relativi alla gestione dei dipendenti/collaboratori, ogni Consociata titolare del rapporto di lavoro è Titolare del trattamento, mentre per i dati personali relativi a clienti e consumatori le Consociate possono configurarsi, a seconda dei casi, come Titolare o Responsabile del trattamento, sulla base di specifici accordi infragrupo sottoscritti fra le stesse (c.d. **“Framework Agreement”**).

Organizzazione HQ Lavazza



3.4 Delegato del Titolare

È riconosciuta al Titolare del trattamento, nella persona del legale rappresentante *pro tempore*, la possibilità di prevedere, sotto la propria responsabilità e nell’ambito del proprio assetto organizzativo, che **specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a soggetti espressamente delegati, che operino sotto la sua autorità**.

Ciò, al fine di meglio garantire il presidio tecnico-specialistico sulla materia ed una qualificata ripartizione interna di compiti e funzioni.

Il Delegato del Titolare del trattamento è, pertanto, la persona fisica designata dal Titolare del trattamento e delegata allo svolgimento delle attività utili a garantire il costante e puntuale rispetto delle normative vigenti in materia di trattamento di dati personali, nonché a rappresentarlo nei rapporti con i soggetti interessati e le Autorità e in tutti gli atti e i contratti di nomina di Terze Parti.

Alla delega, rilasciata con apposita procura speciale, deve essere data adeguata pubblicità, anche interna.

3.5 Responsabile del trattamento (Società del Gruppo e Terze Parti)

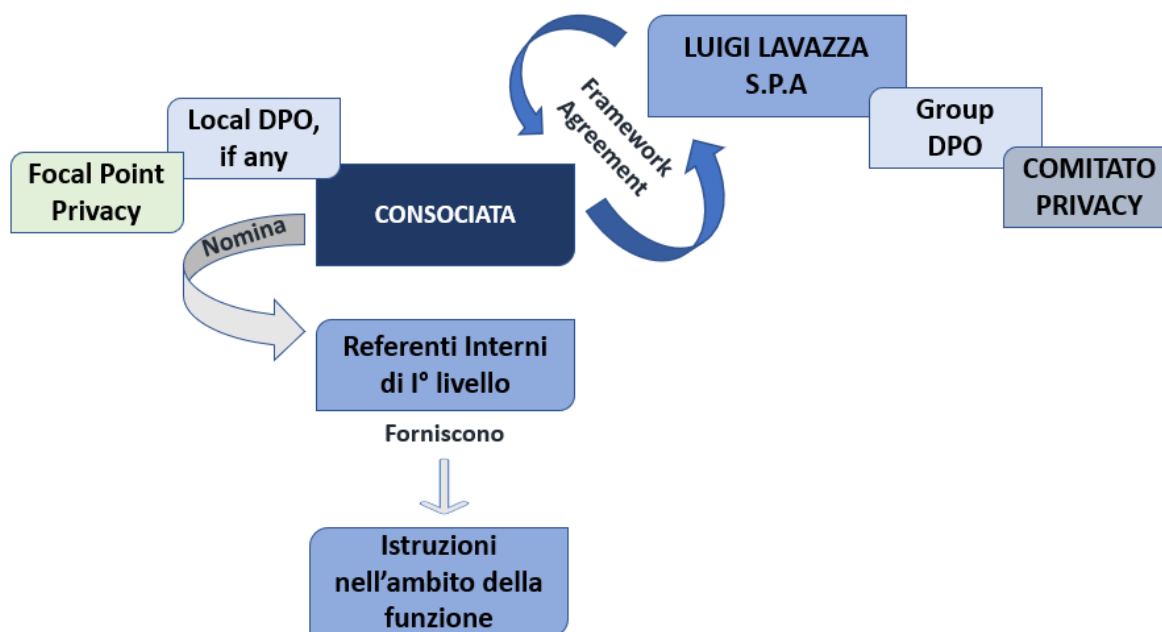
Il Responsabile del trattamento è la persona fisica o giuridica che tratta dati personali per conto del Titolare del trattamento.

I dati personali possono essere trattati in nome e per conto del Titolare del trattamento da parte di società dallo stesso incaricate del loro svolgimento (Società del Gruppo ovvero Terze Parti), previa sottoscrizione di un apposito contratto.

3.5.1 Società del Gruppo

Nell’ambito dell’organizzazione di Gruppo recepita nel M.O.P. (cfr. paragrafo 3.2 che precede), le Consociate, ubicate sia all’interno che all’esterno dell’UE/SEE, sottoscrivono in qualità di **Responsabili del trattamento** appositi accordi per il trattamento dei dati personali (c.d. **“Framework Agreement”** o **“Data Processing Agreement”**) volti a disciplinare – nell’ambito dei **rapporti infragruppo** - la natura, la finalità, la durata del trattamento, il tipo di dati personali, le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento.

Organizzazione Consociate Lavazza (Responsabili del trattamento)



3.5.2 Terze parti

Quando il trattamento viene effettuato da Terze Parti, ovvero da **fornitori, business partner o consulenti che** – in qualità di persone fisiche o giuridiche - **trattano dati personali per conto della società Titolare o Responsabile del trattamento**, l’esecuzione dei trattamenti è disciplinata da un contratto o altro atto giuridico che vincoli la Terza Parte verso la Società e che disciplini almeno: la natura, la finalità, la durata del

trattamento; il tipo di dati personali e le categorie di interessati; il divieto al trasferimento di dati personali all'esterno del perimetro dell'UE; l'applicazione di misure e procedure di sicurezza adeguate; gli obblighi e i diritti del Titolare del trattamento.

Tali soggetti, espressamente identificati quali “**Responsabili del trattamento**” con apposito atto/contratto di nomina (c.d. “**Data Processing Agreement**” o “**DPA**”), dovranno fornire garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse volte a mettere in atto misure tecniche e organizzative adeguate, anche sotto il profilo della sicurezza, al fine di garantire che il trattamento tuteli i diritti degli Interessati.

Il Responsabile del trattamento potrà a sua volta ricorrere ad altro soggetto responsabile (il **Sub-Responsabile**) **previa autorizzazione del Titolare**.

In tutti i casi, il Sub-Responsabile così designato dal Responsabile del trattamento, è tenuto a rispettare gli stessi obblighi stabiliti nel contratto stipulato tra il Titolare e il Responsabile.

3.6. Data Protection Officer

La LUIGI LAVAZZA S.p.A., in qualità di Capogruppo e società “capofila”, ha nominato per tutte le società controllate un *Group Data Protection Officer (DPO)* per il miglior coordinamento a livello di Gruppo degli adempimenti, nonché per il controllo e monitoraggio sull'applicazione delle norme del Regolamento Europeo e delle policy e procedure aziendali adottate in materia di privacy.

Tenuto conto degli obblighi previsti dalle normative locali e delle specifiche attività svolte, possono essere nominati **DPO locali**, che dovranno comunque agire in stretto coordinamento con il DPO individuato a livello di Gruppo, potendo avvalersi del supporto del Comitato Privacy istituito in seno alla Capogruppo.

Eventuali specificità o obblighi normativi suggeriranno, di volta in volta, la nomina di DPO locali.

In linea generale, il DPO di Gruppo ha il compito di:

- informare tempestivamente e fornire consulenza alle Consociate – Titolari o Responsabili del trattamento – in merito al trattamento dei dati personali, avvalendosi del supporto della Funzione Corporate Affairs & Compliance della Capogruppo LUIGI LAVAZZA S.p.A.;
- supportare tutte le funzioni aziendali di Gruppo nella gestione delle tematiche aventi impatto sul trattamento di tali dati;
- sorvegliare sull'osservanza dei requisiti normativi applicabili;
- impostare la compilazione e l'aggiornamento del Registro delle attività del trattamento (cfr. paragrafo 4) per le Società del Gruppo, monitorando i trattamenti con il supporto dei Referenti Interni e degli Autorizzati al trattamento.

Tali compiti vengono svolti dal DPO in **piena autonomia e indipendenza**, caratteristiche garantite dalla circostanza che il DPO **riferisce direttamente al Consiglio di Amministrazione della Capogruppo**, al quale dovrà inviare **periodiche relazioni** sulle principali attività svolte.

La responsabilizzazione richiesta alle Società del Gruppo nel governo e controllo delle tematiche privacy, nonché l'approccio basato sul rischio, comportano la necessità che le valutazioni sui rischi e le adeguate misure tecniche ed organizzative siano adottate sin dalla fase di ideazione e progettazione di ciascun trattamento (c.d. principio della “*Privacy by design*”, cfr. paragrafo 8). Ciascuna funzione aziendale - chiamata ad avviare una nuova attività che possa comportare il trattamento di dati personali o a gestire trattamenti preesistenti con nuove modalità - deve **contattare preventivamente il Group DPO e, ove esistente, il DPO locale per tutti gli approfondimenti e le verifiche su aspetti di compliance**, analisi del rischio e misure di sicurezza.

3.7. Comitato Privacy

Il Comitato Privacy, costituito in seno alla Capogruppo LUIGI LAVAZZA S.p.A., è il gruppo di coordinamento per l'applicazione della normativa privacy composto da rappresentanti delle funzioni aziendali HQ competenti in materia (HR, Internal Audit, Affari Legali e Societari, ICT, Digital Marketing, Marketing Italia e altre di volta in volta individuate) con il compito di supportare la Capogruppo e le sue Consociate nella valutazione di trattamenti di dati personali che possono produrre impatti significativi sulle attività aziendali.

3.8. Focal Point Privacy delle Società del Gruppo LAVAZZA

Per facilitare l'interazione tra il DPO (locale e di Gruppo) e le Società del Gruppo, all'interno di ciascuna Consociata è stato individuato un "**Focal Point Privacy**" (FPP) per la gestione di tutte le tematiche e le specificità locali inerenti al trattamento di dati personali.

Il Focal Point Privacy viene individuato dal General Manager/Regional Director di ciascuna Consociata, con i seguenti compiti:

- aggiornare tempestivamente il DPO locale e di Gruppo su eventuali problematiche, inerenti la protezione dei dati personali, sorte all'interno della Consociata in cui il FP opera, quali ad esempio:
 - possibile Data Breach;
 - distruzione o perdita, anche accidentale, dei dati personali;
 - accesso non autorizzato ai dati personali;
 - nuovi progetti o trattamenti con impatti privacy;
 - problematiche nella gestione dei diritti degli Interessati;
 - nuove Terze Parti coinvolte nel trattamento di dati personali.
- supportare i Referenti Interni della Società nell'analisi del rischio;
- alimentare ed aggiornare periodicamente il Registro dei Trattamenti in collaborazione con il DPO e i Referenti Interni.

3.9 Referenti interni alle Società del Gruppo LAVAZZA

I Referenti Interni sono i soggetti che, responsabili di strutture organizzative aziendali, rappresentano le **figure chiave nel trattamento dei dati personali**.

Nello specifico, il Gruppo LAVAZZA ha individuato come Referenti Interni:

- i primi riporti dell'AD, limitatamente alla LUIGI LAVAZZA S.p.A. ("**Referenti Interni**" di **primo livello**);
- i primi riporti del Titolare (General Manager/Regional Director), con riferimento alle Società del Gruppo (**Referenti Interni di primo livello**);
- i responsabili delle singole funzioni, individuati e nominati dai Referenti Interni di primo livello, che all'interno delle Società del Gruppo trattano dati personali e/o categorie particolari di dati personali ("**Referenti Interni**" di **secondo livello**).

Ciascun Referente Interno, in ragione delle proprie competenze professionali e dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferito, ha il compito di garantire e vigilare sull'attuazione delle misure tecniche, organizzative e di sistema, nonché di supervisionare, anche sulla base delle direttive generali impartite dal Titolare o dal General Manager/Regional Director, lo svolgimento delle operazioni di trattamento effettuate dagli Incaricati che operano nell'ambito della struttura organizzativa di cui è responsabile.

Si indicano qui di seguito i principali ambiti di intervento del Referente Interno:

- collaborare con il Titolare o con il General Manager/Regional Director nell'esecuzione degli adempimenti previsti dalla normativa in materia di privacy;

- dare attuazione ai principi di “*Privacy by Design*” e “*Privacy by Default*” (cfr. paragrafo 8) secondo quanto previsto dal Modello Organizzativo Privacy, coinvolgendo tempestivamente il DPO, anche per il tramite del Focal Point, nelle ipotesi di nuovi trattamenti o nuove modalità di svolgimento di trattamenti preesistenti;
- identificare, nell’ambito della propria funzione, le persone autorizzate al trattamento dei dati personali (“Autorizzati del trattamento”), elaborando e fornendo apposite istruzioni scritte per il trattamento dei dati nell’area di appartenenza;
- supervisionare le operazioni di trattamento svolte dai soggetti autorizzati nella funzione di appartenenza, verificando che vengano eseguite in conformità alle istruzioni impartite;
- monitorare l’applicazione dei processi interni previsti al fine di identificare i trattamenti (nuovi e preesistenti) e verificare il rispetto dei tempi di conservazione dei dati personali definiti dal Titolare, garantendo, qualora previsto, che cancellazione e/o anonimizzazione dei dati avvengano in modo conforme alle prescrizioni impartite;
- con riferimento al trattamento dei dati effettuato all’interno della funzione di competenza, alimentare ed aggiornare periodicamente il Registro dei Trattamenti con la collaborazione del team DPO;
- contattare/coinvolgere tempestivamente il Group DPO, e il DPO locale ove presente, il Focal Point Privacy nel caso di richieste e/o reclami di terzi inerenti alla protezione dei dati personali;
- supportare il DPO di Gruppo/locale ed il Titolare nella rilevazione e gestione di potenziali violazioni dei dati personali (Data Breach), garantendo la necessaria collaborazione nelle attività di *recovery* che dovessero essere individuate (investigazione, mitigazione ed eliminazione delle conseguenze derivanti dalla violazione) e di aggiornamento del Registro delle violazioni.

3.10 Autorizzati al trattamento

Gli Autorizzati al trattamento, ossia le persone autorizzate allo svolgimento di operazioni di trattamento di dati personali, operano sulla base di apposite istruzioni scritte fornite dal proprio Referente Interno per il trattamento dei dati nell’area di appartenenza.

Ciascun Autorizzato deve limitarsi a trattare dati personali **in funzione di quanto strettamente necessario** in relazione all’**esercizio delle proprie mansioni ed in conformità con le indicazioni operative ricevute**, sotto l’autorità diretta del Titolare.

Al fine di una gestione responsabile e conforme alle leggi e ai regolamenti esistenti, gli Autorizzati al trattamento che raccolgono, utilizzano e conservano dati personali devono nella propria area di appartenenza:

- mantenere i dati personali in modo accurato e aggiornato, dalla raccolta alla distruzione;
- proteggere i dati personali in modo che non siano accessibili ad un numero indefinito di persone o comunque a soggetti che non siano autorizzati o che non abbiano una valida ragione di business per accedere alle informazioni;
- impedire l’utilizzo illecito o improprio dei dati personali, qualora il loro utilizzo non sia compatibile con la finalità per la quale i dati sono stati raccolti;
- assicurare la tracciabilità e rintracciabilità dei dati personali (accessi, modifiche, archiviazione) durante tutto il loro ciclo di vita;
- conservare i dati personali solo per la durata necessaria allo scopo indicato e/o per il tempo previsto dalle norme e/o regolamenti vigenti, o comunque in conformità alle istruzioni impartite;
- riferire tempestivamente qualsiasi violazione della Privacy (accesso non autorizzato ai sistemi, perdita, smarrimento, furto, distruzione o cancellazione di dati) oltre che al Service Desk IT, anche e tempestivamente al “Focal Point” locale, al proprio Referente Interno e – nei casi più gravi - al DPO locale e di Gruppo;

- evitare di conservare dati personali su file non protetti da password e/o su memorie esterne o laptop, il cui smarrimento o furto potrebbero determinare una violazione di dati personali (“Data Breach”);

nonché collaborare con il DPO e con il proprio Referente Interno nella compilazione ed aggiornamento periodico del Registro dei Trattamenti.

3.10.1 Autorizzati al trattamento di videosorveglianza

L’Autorizzato al trattamento del sistema di Videosorveglianza è il soggetto che, preposto alla *Security* aziendale, è autorizzato dal Titolare/Responsabile o dal Referente Interno della Consociata a compiere **operazioni di trattamento sulle immagini, registrate e non, rilevate dai sistemi di videosorveglianza installati presso le sedi della Società per finalità di protezione del patrimonio aziendale.**

Qualora, nell’ambito di un contratto di servizi di vigilanza con la Società, un soggetto terzo venga autorizzato a compiere per conto del Gruppo LAVAZZA operazioni di trattamento sulle immagini raccolte dall’impianto di videosorveglianza, questi dovrà essere nominato “Responsabile del trattamento”.

Le Società del Gruppo LAVAZZA effettuano trattamento di dati personali tramite sistemi di videosorveglianza installati presso le proprie sedi e stabilimenti e sono, pertanto, tenute all’adozione delle prescrizioni normative applicabili in materia di videosorveglianza⁹.

4. Registro delle attività di trattamento

In ottemperanza alle disposizioni del Regolamento europeo, ogni Società del Gruppo che tratta dati personali è tenuta a compilare il **Registro delle attività di trattamento** effettuate sotto la sua responsabilità. Il Registro, redatto in forma scritta, anche in formato elettronico, deve essere tenuto a disposizione dell’autorità competente.

La Capogruppo LUIGI LAVAZZA S.p.A. si è dotata di un unico tool di Gruppo dedicato alla tenuta del Registro dei trattamenti effettuati da ciascuna Società del Gruppo e nel quale sono mappati i singoli trattamenti effettuati nell’ambito delle Direzioni e Funzioni aziendali, le richieste degli interessati, le valutazioni di impatto, i Responsabili del trattamento ed i relativi DPA, etc.

Il Registro dei Trattamenti è **parte integrante del sistema di corretta gestione dei dati personali e del M.O.P.**; viene alimentato ed aggiornato periodicamente per ciascuna Società del Gruppo.

5. Modello di gestione

Le operazioni di trattamento di dati personali devono avvenire in modo **lecito, corretto e trasparente**, strettamente limitato a quanto necessario a perseguire le finalità indicate nell’informativa privacy e, in ogni caso, compatibili con dette finalità.

Si possono individuare tre fasi del “ciclo di vita” del dato personale:

- Raccolta;
- Trattamento;
- Cessazione del Trattamento e Cancellazione.

⁹ Provvedimento del Garante della protezione dei dati personali in materia di videosorveglianza dell’8 aprile 2010, nonché Linee guida 3/2019 sulla videosorveglianza dell’European Data Protection Board (EDPB)

5.1 Raccolta

5.1.1 Finalità

Il Trattamento dei dati personali (raccolti o ricevuti) da parte delle Società del Gruppo LAVAZZA deve avvenire per il **perseguimento di finalità legittime**.

I dati personali raccolti devono essere **adeguati, pertinenti e limitati** a quanto necessario per le finalità del loro trattamento.

Si riportano qui di seguito, a mero titolo esemplificativo, talune finalità:

- gestione della relazione con clienti e fornitori (persone fisiche);
- selezione e assunzione del personale e gestione del rapporto di lavoro con il medesimo;
- invio di materiale pubblicitario e altre iniziative promozionali e di marketing;
- attività di vendita diretta;
- analisi su abitudini e scelte di consumo ed elaborazioni statistiche;
- attività di profilazione;
- gestione degli accessi alle sedi delle Società del Gruppo e videosorveglianza.

5.1.2 Base giuridica

Ciascun trattamento di dati personali richiede l'identificazione della **base giuridica a giustificazione del trattamento**, vale a dire la ragione che legittima il trattamento dei dati personali.

Per quanto riguarda i dati personali trattati nell'ambito del Gruppo LAVAZZA, le **basi giuridiche** del trattamento sono:

- **il consenso dell'interessato**: quando il trattamento dei dati viene esplicitamente autorizzato dall'interessato per una o più specifiche finalità (ad esempio, per usare i dati dell'interessato per finalità di marketing)
- **l'esecuzione di un contratto o di previsioni precontrattuali**: quando il trattamento è necessario per adempiere ad un contratto voluto dall'interessato (ad esempio, per spedire dei i acquistati da un cliente occorrerà raccogliere i suoi dati personali come nome, cognome, indirizzo, etc.)
- **l'adempimento ad un obbligo di legge**: quando il trattamento dei dati è imposto da una legge, regolamento, etc. (ad esempio, per fatturare l'acquisto di un bene al cliente occorre raccogliere i suoi dati fiscali, etc.)
- **interesse legittimo del Titolare**: quando il trattamento è necessario per esigenze specifiche del Titolare a condizione però che il trattamento non sia eccessivamente invasivo per l'interessato (ad esempio, per installare un sistema di videosorveglianza per fini di sicurezza).

5.1.2.1 Il consenso

Il consenso, laddove necessario quale **presupposto di liceità del trattamento**, deve essere espresso mediante un atto positivo con il quale l'Interessato manifesta l'**intenzione libera, specifica, informata e inequivocabile** di accettare il trattamento dei dati personali che lo riguardano, mediante **dichiarazione scritta** (anche attraverso mezzi elettronici, ad es. la selezione di un'apposita casella in un sito web) o **orale**.

Il silenzio, l'inattività o la preselezione di caselle non equivale a prestare il consenso.

Il consenso è considerato **liberamente espresso** se l'Interessato è in grado di operare una scelta autenticamente libera ed è nella possibilità di rifiutare o revocare il consenso senza subire pregiudizio. Si presume che il consenso non sia liberamente espresso se:

- l'esecuzione di un contratto, o la prestazione di un servizio, sono subordinati alla prestazione di un consenso che non sarebbe peraltro necessario per l'esecuzione di tale contratto;
- o se non è possibile esprimere un consenso separato per distinti trattamenti di dati personali.

È necessario infatti che venga richiesto, in forma comprensibile e facilmente accessibile, un **consenso esplicito per ogni specifica finalità di trattamento**. Qualora il trattamento abbia **più finalità**, il consenso deve essere espresso per ciascuna di esse¹⁰.

L'onere della prova circa l'avvenuto consenso è in capo al Titolare (e/o al Responsabile del Trattamento), il quale deve essere in grado di dimostrare che l'Interessato ha espressamente acconsentito al trattamento dei dati.

Nel caso di raccolta **orale** del consenso (ad es. nello svolgimento di attività di marketing telefonico affidata a *call center*), gli operatori cui è demandato il compito di contattare liste di nominativi e gestire il colloquio telefonico finalizzato ad attività promozionali e/o di raccolta di informazioni, dovranno espressamente utilizzare gli *script* appositamente predisposti (per l'Informativa privacy e la raccolta dei consensi, provvedendo a registrare, trascrivere e a documentare per iscritto gli avvenuti consensi).

Il consenso degli Interessati **non è necessario** per lo svolgimento di talune operazioni di trattamento, ovvero per:

- l'esecuzione di un contratto di cui l'Interessato è parte o esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- l'adempimento di un obbligo legale cui è soggetto il Titolare;
- il perseguimento del legittimo interesse del Titolare, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato.

Si citano qui di seguito, a mero titolo esemplificativo, alcune delle finalità per le quali è necessario raccogliere specifico consenso:

- invio di materiale pubblicitario e altre iniziative promozionali e di marketing;
- attività di profilazione ovvero trattamenti volti ad analizzare preferenze, abitudini e scelte di consumo¹¹;
- attività concernenti il trattamento di speciali categorie di dati, i c.d. **dati particolari** (dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale; dati genetici; dati biometrici; dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona), nonché il trattamento di **dati personali relativi a condanne penali e reati**, ove richiesto dalla legge.

Gli Interessati hanno la possibilità di **revocare**, in qualsiasi momento, il consenso precedentemente prestato allo svolgimento di determinate operazioni di trattamento.

In tali ipotesi, le operazioni di trattamento svolte in virtù di tale consenso dovranno essere **prontamente interrotte** salvo che sussista altro fondamento giuridico per il trattamento (tra i

¹⁰ Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'Interessato, occorre che il trattamento per l'ulteriore e diversa finalità sia **compatibile** con la finalità per la quale i dati personali sono stati inizialmente raccolti (tenuto conto del nesso tra le finalità, del contesto in cui i dati sono stati raccolti, della natura dei dati, delle possibili conseguenze dell'ulteriore trattamento e dell'esistenza di garanzie adeguate).

¹¹ La **profilazione** è una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'Interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona.

quali, ad es., adempimento di un obbligo legale; difesa di un diritto in sede giudiziaria; condizioni di legittimo interesse del Titolare che siano prevalenti rispetto agli interessi, ai diritti ed alle libertà fondamentali dell'Interessato).

In tutti i casi, consensi e revoche devono essere opportunamente tracciati, per poter eventualmente documentare le modifiche/variazioni richieste degli Interessati.

5.1.2.2 Esecuzione di un contratto

Quando il trattamento dei dati personali è **necessario** all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso, il trattamento dei dati personali può lecitamente fondarsi sulla base giuridica dell'esecuzione di un contratto.

Essendo il **criterio di necessità** fondamentale per questa base giuridica, il trattamento dei dati sarà lecito solo ove il contratto non possa essere integralmente eseguito senza il trattamento dei dati personali (per esempio, ai fini della sottoscrizione di un contratto occorre necessariamente richiedere i dati identificativi dell'interessato). Tale circostanza determina, conseguentemente, l'impossibilità di avvalersi di tale base giuridica laddove i dati non siano necessari alla sottoscrizione del contratto (per es. per finalità di marketing).

Perché il trattamento fondato su tale base giuridica sia considerato lecito occorrerà **dimostrare**:

- l'esistenza del contratto fra l'azienda e il soggetto interessato;
- la validità dello stesso contratto;
- che il trattamento di quei dati forniti dall'interessato sia oggettivamente necessario per l'esecuzione del contratto.

È sempre necessario **fornire l'informativa privacy** che indichi la base giuridica del trattamento.

5.1.2.3 Adempimento di un obbligo di legge

Tale base giuridica trova applicazione quando il trattamento dei dati personali è necessario per **l'adempimento di obblighi derivanti dalla legge**.

È il caso di trattamenti di dati personali necessari per la gestione degli adempimenti amministrativi e fiscali posti in capo alle aziende nell'ambito dei rapporti di lavoro (per esempio, gestione dei cedolini paga, etc.).

L'obbligo legale, tuttavia, deve soddisfare quattro condizioni:

- Deve essere **definito dalla legge** europea o nazionale di uno Stato;
- Tali disposizioni legali devono stabilire un **obbligo imperativo di trattamento dei dati personali**, sufficientemente chiaro e preciso;
- Tali disposizioni devono almeno definire le finalità del trattamento in questione;
- Tale obbligo deve essere imposto al Titolare del trattamento e non alle persone interessate dal trattamento.

In questi casi non occorre il consenso dell'interessato, ma è opportuno fornire comunque l'informativa privacy in cui viene indicata la base giuridica del trattamento.

5.1.2.4 Legittimo interesse

Laddove il trattamento dei dati personali sia necessario al perseguimento del **legittimo interesse** del Titolare del trattamento e a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, i dati personali possono essere trattati senza il previo consenso dell'interessato.

Per poter fondare il trattamento su tale base giuridica, tuttavia, occorre effettuare un bilanciamento fra gli interessi del Titolare e dei diritti riconosciuti al soggetto interessato dalla normativa vigente in materia di trattamento dei dati personali al fine valutare e dimostrare la prevalenza degli interessi del Titolare sui diritti dell'interessato. Nel fare il **bilanciamento di interessi** (c.d. "*Legitimate Interest Assesment*" o "LIA") occorre valutare:

- se il **trattamento sia realmente necessario** tenendo conto del **possibile pregiudizio** che ne deriverebbe al Titolare qualora non effettuasse il trattamento;
- l'**impatto sugli interessati** e la loro **ragionevole aspettativa** riguardo a ciò che accadrà ai loro dati personali;
- la **presenza di misure aggiuntive di protezione dei dati** che possano limitare gli impatti del trattamento sugli interessati.

Le Società del Gruppo sono tenute a condurre tale bilanciamento di interessi ogni qualvolta il trattamento dei dati personali si fonda sul legittimo interesse, con il supporto del DPO di Gruppo e/o locale, ove presente.

5.1.3 L' informativa privacy

I principi di trattamento corretto e trasparente implicano che l' Interessato sia informato dell' esistenza del trattamento e delle sue finalità.

Il Titolare del trattamento deve fornire all' Interessato tutte le informazioni relative al trattamento dei dati personali che lo riguardano, in forma **concisa, comprensibile e facilmente accessibile**, con **linguaggio semplice e chiaro**, per iscritto o con altri mezzi, anche in formato elettronico (sito web).

Le modalità con cui i dati personali sono raccolti, utilizzati, consultati o altrimenti trattati devono essere **trasparenti** per gli Interessati. In particolare, le finalità specifiche del trattamento dei dati personali devono essere **esplicite e legittime** e precisate al momento della raccolta dei dati.

L' informativa privacy¹² deve essere fornita all' Interessato **al momento della raccolta** dei dati personali o, se i dati sono ottenuti da altra fonte, **entro un termine ragionevole** ma, al più tardi, **entro un mese**. Nel caso in cui i dati personali siano destinati alla comunicazione con l' Interessato o con altro destinatario, l' Informativa privacy deve essere fornita al più tardi al momento della prima comunicazione dei dati.

In caso di dati raccolti direttamente presso l' Interessato, questi deve essere informato dell' eventuale obbligo di fornire i dati personali e delle conseguenze in cui incorre in caso di rifiuto a fornirli.

Nelle ipotesi di nuovi trattamenti o nuove modalità di svolgimento di trattamenti preesistenti, sarà responsabilità di ciascuna funzione aziendale contattare preventivamente il DPO, anche per il tramite del Focal Point Privacy, per tutti gli approfondimenti e le verifiche sugli aspetti di compliance (normativa, analisi del rischio e di sicurezza).

5.2 Trattamento – Principi generali

Le operazioni di trattamento effettuate dalle Società del Gruppo LAVAZZA devono attenersi ai principi generali dettati dalle norme e riportati di seguito:

¹² Il Gruppo LAVAZZA informa tutti gli Interessati relativamente:

- alla tipologia di dati personali trattati;
- alla finalità per le quali i dati personali sono raccolti e la base giuridica del trattamento;
- alla natura del conferimento;
- alle modalità di trattamento dei dati;
- alle modalità di comunicazione e trasferimento dei dati;
- al periodo di conservazione dei dati;
- al trattamento di dati di minori;
- ai diritti degli Interessati e relative modalità di esercizio.

- **Liceità, correttezza e trasparenza:** i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato;
- **Limitazione delle finalità:** i dati devono essere raccolti per finalità determinate, esplicite e legittime, specificatamente dichiarate e descritte in modo chiaro e comprensibile nell'Informativa, e successivamente trattati con modalità non incompatibili con tali finalità. Non è consentito l'utilizzo dei dati raccolti per finalità diverse da quanto dichiarato nell'Informativa: qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui sono stati inizialmente raccolti, prima di tale ulteriore trattamento dovrà fornire all'Interessato una nuova Informativa e, se del caso, interessato dovrà raccogliere un nuovo esplicito consenso;
- **Minimizzazione dei dati:** i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- **Esattezza:** i dati devono essere esatti e, se necessario, aggiornati. Bisogna adottare tutte le misure ragionevoli per rettificare o cancellare tempestivamente i dati personali inesatti;
- **Limitazione della conservazione:** i dati devono essere conservati in una forma che consenta l'identificazione dell'Interessato per un periodo di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono stati trattati;
- **Integrità e riservatezza:** i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione - mediante misure tecniche e organizzative adeguate - da trattamenti non autorizzati o illeciti e dalla perdita, distruzione, modifica, rivelazione o accesso non autorizzati che potrebbero cagionare un danno.

5.2.1 Trattamento effettuato da Terze Parti

Per trattamento di dati personali effettuato da Terze Parti si intendono tutte le casistiche in cui dati di titolarità di Società del Gruppo LAVAZZA, o per i quali le Società del Gruppo siano state designate Responsabili del trattamento, siano resi in qualsiasi modo accessibili, anche tramite connessione remota, a Terze Parti.

In questi casi troveranno applicazione le disposizioni di cui al paragrafo 3.5.

5.2.2 Trasferimenti transfrontalieri di dati personali– Flussi infragruppo

Con i trasferimenti transfrontalieri di dati personali al di fuori dell'UE/SEE potrebbe aumentare il rischio che l'Interessato non possa esercitare il proprio diritto alla protezione dei dati, in particolare per tutelarsi da usi e comunicazioni illecite di tali informazioni.

È opportuno che quando i dati personali sono trasferiti dall'UE/SEE a Titolari o Responsabili del trattamento in paesi terzi (extra UE/SEE), il livello di tutela delle persone fisiche assicurato in ambito UE dal Regolamento europeo non sia compromesso, anche nei casi di successivi trasferimenti di dati personali dal paese terzo verso altri paesi terzi.

Il trasferimento di dati personali verso un paese terzo (da intendersi come ogni ipotesi in cui i dati siano accessibili in uno stato estero, anche tramite il semplice accesso da remoto) può avvenire solo al fine di perseguire la finalità comunicata all'Interessato al momento della raccolta e in conformità alle specifiche disposizioni riguardanti il trasferimento di dati personali all'estero.

Il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati ad essere oggetto di un trattamento dopo il trasferimento può avvenire verso paesi che – su decisione della Commissione europea - garantiscano un adeguato livello di protezione (trasferimento sulla base di una **decisione di adeguatezza**).

In mancanza di una decisione di adeguatezza, e fatti salvi i casi in cui il trasferimento è consentito per legge (tra cui il consenso inequivocabile della persona interessata; la necessità del trasferimento per l'esecuzione di misure contrattuali/precontrattuali; la necessità del trasferimento per l'esercizio o la difesa di un diritto in sede giudiziaria), il Titolare del trattamento deve provvedere a compensare la carenza di protezione, connessa al trasferimento dei dati personali verso paesi terzi, con **adeguate garanzie** a tutela degli Interessati, comprese la disponibilità di diritti azionabili dagli Interessati e mezzi di ricorso effettivi, attraverso alternativamente:

- le **norme vincolanti di impresa** (c.d. *Binding Corporate Rules - BCR*), approvate da un'autorità di controllo, volte a consentire il trasferimento di dati personali dal territorio dello Stato verso paesi terzi tra società facenti parte dello stesso gruppo imprenditoriale. Si concretizzano in un documento contenente una serie di clausole (*rules*) che fissano i principi vincolanti (*binding*) al cui rispetto sono tenute tutte le società appartenenti ad uno stesso gruppo (*corporate*)^{13 14};
- le **Clausole Contrattuali Standard** (c.d. *Standard Contractual Clauses- SCC*) adottate dalla Commissione o adottate da un'autorità di controllo e approvate dalla Commissione;
- le **clausole contrattuali modello (ad hoc)** autorizzate da un'autorità di controllo;
- I **codici di condotta** sono regole di condotta o pratiche uniformi elaborate da vari organismi internazionali o anche da singoli Stati, destinati a contribuire alla corretta applicazione del Regolamento, in funzione delle specificità settoriali e delle esigenze specifiche delle micro, piccole e medie imprese.
- I **meccanismi di certificazione** sono forme di accreditamento che permettono di ottenere il rilascio di un'attestazione da una parte terza (organismo di certificazione - OdC) allo scopo di dimostrare la conformità, al Regolamento Generale per la Protezione dei Dati Personali (GDPR), dei trattamenti effettuati.


5.2.3 Cookies e tecnologie similari

I siti web delle Società del Gruppo LAVAZZA possono utilizzare *cookies* o tecnologie ad essi assimilabili per attività di **profilazione e di marketing**, in particolare al fine di analizzare o prevedere aspetti riguardanti le preferenze, abitudini o scelte di consumo o gli interessi personali dell'Interessato e di fornire servizi o contenuti pubblicitari mirati, di mostrare contenuti e proporre iniziative commerciali.

I cookies, eccetto quelli necessari che consentono il normale funzionamento dei siti web, possono essere utilizzati previo consenso dei soggetti interessati. Il consenso viene acquisito attraverso l'apertura di un banner visibile agli utenti alla prima visita del sito con il quale gli interessati vengono invitati ad esprimere le loro preferenze in merito all'utilizzo dei cookies, c.d. **cookie manager**.

¹³ Le BCR costituiscono un meccanismo in grado di semplificare gli oneri a carico delle società di carattere multinazionale con riferimento ai flussi infragruppo di dati personali. Il rilascio di un'autorizzazione (da parte del Garante per la protezione dei dati personali) al trasferimento di dati personali (dall'Italia verso paesi terzi) tramite Binding Corporate Rules consente infatti alle società del gruppo multinazionale che ne abbia fatto richiesta, anche se stabilite in diversi paesi, di trasferire all'interno del gruppo d'impresa i dati personali senza necessità di ulteriori adempimenti, purché nel rispetto di quanto stabilito all'interno del testo delle BCR e per le sole finalità ivi indicate.

¹⁴ Sono previsti alcuni oneri in capo al gruppo multinazionale che ricorre alle BCR, tra cui: la predisposizione di un programma di training del personale in materia di protezione dei dati personali; l'implementazione di un meccanismo di gestione del contenzioso e delle segnalazioni connesse alle BCR; la conduzione periodica di audit al fine di verificare il rispetto delle BCR da parte delle società del Gruppo; la creazione di uno staff che si occupi di monitorare il rispetto delle BCR e di gestire le segnalazioni degli Interessati.

A decorative graphic in the top left corner consisting of several coffee beans and a yellow circle, with thin yellow lines connecting them.

Il cookie manager, oltre a consentire agli utenti di fornire o negare i consensi per categorie di cookies consente altresì loro di avere informazioni granulari sulle categorie di cookie ovvero in relazione a ciascun singolo cookie quali finalità del cookie, durata, categoria (tecnici, analitici, marketing, profilazione).

Il consenso, laddove fornito, viene acquisito in maniera lecita (per i requisiti di validità del consenso si veda la sezione 5.1.3 ad esso dedicata) e viene tracciato per documentare la scelta del soggetto interessato.

5.2.4 Sicurezza

Nell'ambito delle operazioni di trattamento svolte, le Società del Gruppo mettono in atto misure per garantire un **livello di sicurezza adeguato al rischio**.

In particolare, i dati personali devono essere trattati in modo da garantire un'**adeguata sicurezza** compresa la protezione - mediante misure tecniche e organizzative adeguate - da trattamenti non autorizzati o illeciti e dalla perdita, distruzione, modifica, rivelazione o accesso non autorizzati.

Tenuto conto dello stato dell'arte, dei costi di attuazione rispetto ai rischi che presentano i trattamenti e della natura dei dati personali da proteggere, vengono attuate in particolare le seguenti misure:

- controlli fisici agli accessi;
- restrizioni al solo personale autorizzato per specifiche aree sensibili (archivio Risorse Umane, Control Room, impianti di videosorveglianza)
- distruzione sicura della documentazione cartacea contenente dati personali;
- cancellazione sicura dei supporti informatici che, utilizzati per il trattamento dei dati, siano destinati ad altro uso;
- pseudonimizzazione o cifratura dei dati personali;
- tempestivo ripristino della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico;
- implementazione di misure di protezione delle reti, dei sistemi e dei software con i quali vengono trattati i dati personali;
- applicazione del principio di Privacy *by design* e *by default* (cfr. paragrafo 8) nella progettazione dei sistemi e nel disegno dei processi e delle procedure aziendali;
- processi, strumenti e organizzazione per assicurare la tempestiva segnalazione di eventuali tentativi non leciti di accesso ai dati personali;
- procedure per la gestione delle violazioni (Data Breach);
 - adozione di soluzioni per il tracciamento delle attività effettuate sui dati personali;
 - adeguate prassi operative per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

5.3 Trattamenti specifici - Cessazione del Trattamento - Cancellazione e Distruzione

Le Società del Gruppo interessate dall'applicazione della presente Policy devono:

- adottare tutte le misure ragionevoli per **cancellare o rettificare tempestivamente i dati inesatti** rispetto alle finalità per le quali sono trattati;
- assicurare che il **periodo di conservazione dei dati personali sia limitato al minimo necessario**, in relazione alle specifiche finalità della raccolta e del trattamento.

Onde assicurare che i dati personali non siano conservati più a lungo del necessario, occorre che sia stabilito un **termine per la cessazione del trattamento e per la cancellazione**.

Il periodo di conservazione dei dati, nonché i criteri utilizzati per definire tale periodo in relazione alle diverse attività di trattamento riportate nel Registro dei trattamenti, è definito nelle Linee Guida dedicate_ *Data Retention per Gruppi di trattamento*.

Nel caso in cui una Società del Gruppo intenda cessare lo svolgimento di una o più operazioni di trattamento, i dati personali (in formato cartaceo ed elettronico) precedentemente utilizzati nel contesto di tali operazioni, fermo il periodo di conservazione di cui sopra e fatti salvi gli adempimenti legati ad obblighi di legge o a finalità connesse all'esercizio o alla difesa di un diritto in sede giudiziaria, dovranno essere **cancellati**.

Il Gruppo LAVAZZA garantirà, in particolare, che i supporti informatici vengano opportunamente formattati in caso di assegnazione di pc (fisso o portatile) o telefono cellulare ad altro dipendente, nonché, in caso di dismissione di tali apparecchiature per fine vita, a procedure di cancellazione sicura o distruzione per prevenire la diffusione, anche accidentale, di dati.

6. Diritti dell'interessato e riscontro

L'Interessato ha diritto di accedere ai dati personali che lo riguardano e di esercitare tale diritto facilmente, per essere consapevole del trattamento e verificarne la liceità.

In particolare, ogni Interessato ha diritto di conoscere e ottenere comunicazioni in relazione:

- alle finalità per cui e al periodo in cui i dati personali sono trattati;
- ai destinatari dei dati personali;
- alla logica cui risponde ogni trattamento automatizzato dei dati e alle possibili conseguenze di un'eventuale profilazione.

Le Società del Gruppo agevolano e non possono rifiutarsi di soddisfare la richiesta di esercizio dei diritti degli Interessati, salvo che dimostri di non essere in grado di identificare l'interessato.

All'interessato devono essere fornite le informazioni oggetto di richiesta **senza ingiustificato ritardo** e comunque, al più tardi, **entro un mese** dal ricevimento della richiesta stessa, salvo proroga – nei casi consentiti dalla legge – tenuto conto della complessità e del numero delle richieste.

Di seguito vengono riportati i diritti degli Interessati previsti dalla normativa di tutela dei dati personali.

6.1 Diritto di accesso

L'Interessato ha il diritto di ottenere la conferma che sia o meno in corso un trattamento dei dati personali che lo riguardano e, in tal caso, di ottenere l'accesso e una copia dei dati oggetto di trattamento.

6.2 Diritto di rettifica

L'Interessato ha il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo, nonché l'integrazione dei dati personali incompleti, fornendo una dichiarazione integrativa.

6.3 Diritto alla cancellazione

L'Interessato ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano e il Titolare ha l'obbligo di cancellarli senza ingiustificato ritardo, se sussiste uno dei seguenti motivi:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- l'Interessato revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per il trattamento (tra cui, ad es., adempimento di un obbligo legale; difesa di un diritto in sede giudiziaria; condizioni di legittimo interesse del Titolare che siano prevalenti rispetto agli interessi, ai diritti ed alle libertà fondamentali dell'Interessato);
- l'interessato si oppone al trattamento dei dati personali che lo riguardano;
- i dati personali sono trattati illecitamente.

6.4 Diritto di limitazione al trattamento

L'Interessato ha il diritto di ottenere la limitazione del trattamento quando, tra gli altri casi:

- contesta l'esattezza dei dati personali, per il periodo necessario al Titolare per verificare l'esattezza di tali dati;
- quando, a fronte di un trattamento illecito, l'Interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo.

Le modalità per limitare il trattamento dei dati personali possono consistere nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, o nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web.

6.5 Diritto alla portabilità dei dati

L'Interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano e che ha fornito e di trasmetterli a un altro Titolare del trattamento senza impedimenti, qualora:

- il trattamento si basi sul consenso o se il trattamento è necessario per l'esecuzione di un contratto di cui l'Interessato è parte; e
- il trattamento sia effettuato con mezzi automatizzati.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'Interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un Titolare del trattamento all'altro, se tecnicamente fattibile. Qualora un certo insieme di dati personali riguardi più di un interessato, il diritto alla portabilità dei dati non deve pregiudicare i diritti e le libertà degli altri interessati.

6.6 Diritto di opposizione

L'Interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano.

L'esercizio di tale diritto determina l'astensione dal trattare ulteriormente i dati personali, salvo che non venga dimostrato che vi siano motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'Interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Qualora i dati personali siano trattati per finalità di marketing diretto, l'Interessato ha il diritto di opporsi - in qualsiasi momento e gratuitamente - a tale trattamento, ivi compresa la profilazione connessa alla finalità di marketing diretto.

6.7 Risposta al richiedente e termini previsti

Prima del riscontro all'esercizio dei diritti, è indispensabile che la Società del Gruppo adotti tutte le misure ragionevoli volte a verificare l'identità dell'Interessato, o del soggetto che formula la richiesta per conto di questi, in particolare nel contesto di servizi online o di identificativi online, richiedendo – se del caso - copia di un documento di identità in corso di validità.

Se la richiesta proviene da persona che agisce per conto dell'interessato è necessario verificare:

- la delega firmata dall'Interessato;
- l'identità dell'Interessato e del soggetto delegato.

Se la richiesta riguarda l'accesso ai dati di una persona deceduta, è necessario identificare il richiedente e accertarsi che si tratti di un erede, o comunque, di persona legittimata all'esercizio del diritto.

È opportuno tracciare la risposta fornita all'Interessato o alla persona da lui delegata.

Qualora le richieste vengano indirizzate direttamente al Customer Service o al Contact Center, sarà compito del Customer Service verificare lo storico dei dati trattati (raccolta, uso, archiviazione, cancellazione), dare corso alle richieste degli Interessati e confermare agli stessi l'esito delle richieste.

Laddove sorgessero dubbi nell'interpretazione delle richieste pervenute, nel rigoroso rispetto dei tempi di risposta previsti dalla norma, è opportuno che il Responsabile del Customer Service coinvolga il DPO in modo da concordare e definire il corretto intervento da attuare.

Nel solo caso di richieste indirizzate direttamente dagli Interessati al DPO attraverso il canale dedicato (indirizzo e-mail privacyDPO@LAVAZZA.com), sarà quest'ultimo a coinvolgere il Customer Service per le necessarie verifiche e ad autorizzare gli interventi del caso, dandone direttamente conferma agli Interessati.

7. Istruzioni operative

Ogni Società del Gruppo LAVAZZA, per far fronte alle richieste che possono pervenire dagli Interessati, in modo particolare da clienti e/o consumatori, a fronte dei diritti riportati al paragrafo 6, rende noti agli Interessati, sui siti istituzionali delle Società del Gruppo, l'indirizzo e-mail del DPO (privacyDPO@lavazza.com) e del DPO locale, ove presente, oltre che del Contact Center per le attività gestite dal Servizio Consumatori.

8. Privacy by design & by default

Il principio di responsabilizzazione comporta che questi sia in grado di dimostrare la conformità al Regolamento europeo attraverso l'adozione - sin dalla fase di ideazione e progettazione dell'attività di trattamento di dati personali ("**Privacy by design**") - di adeguate misure tecniche e organizzative e di politiche interne idonee a garantire che siano trattati, per impostazione predefinita ("**Privacy by default**"), solo i dati personali necessari (per quantità, portata del trattamento, periodo di conservazione e accessibilità) per ogni specifica finalità del trattamento.

Tali misure consistono, tra l'altro, nel ridurre al minimo il trattamento di dati personali, nel pseudonimizzare i dati personali nel minor tempo possibile, nel consentire agli Interessati di controllare il trattamento dei propri dati, nel creare e migliorare le caratteristiche di sicurezza, nel definire chiare ripartizioni di responsabilità interne.

Con il fine ultimo di implementare soluzioni di progettazione dei trattamenti di dati personali, dei processi e dei sistemi informativi in grado di proteggere i dati durante tutte le fasi del "ciclo di vita", il Gruppo LAVAZZA

mette in atto misure tecniche e organizzative per garantire in modo preventivo la protezione dei dati trattati, assicurando il rispetto dei seguenti principi:

- responsabilità nel trattamento dei dati da parte di tutti i collaboratori del Gruppo e dei business partners, al fine di salvaguardare la confidenzialità, l'integrità e la disponibilità dei dati personali trattati;
- informazione agli Interessati circa le modalità con cui LAVAZZA raccoglie, utilizza, conserva e comunica i dati personali;
- utilizzo e conservazione dei dati esclusivamente per le finalità dichiarate agli Interessati ed espressamente autorizzate dal loro consenso esplicito;
- trasferimento dei dati ai business partners solo per le finalità identificate nell'informativa e con un adeguato livello di sicurezza;
- accesso limitato ai dati da parte di personale autorizzato e formato alla gestione dei dati personali;
- monitoraggio sulla corretta applicazione, sia interna che esterna, dei principi e delle indicazioni fornite nella presente Policy.

L'approccio di *Privacy by Design e by Default* deve considerare l'intero "ciclo di vita" dei dati personali, dalla raccolta alla cancellazione, tenendo in debita considerazione qualsiasi operazione di trattamento dei dati (registrazione, conservazione, consultazione, uso, comunicazione, trasferimento) e salvaguardandone la confidenzialità, integrità e disponibilità, in tutti i processi/sistemi/applicativi attraverso i quali vengono trattati dati personali.

Tali principi devono essere integrati nell'intera organizzazione del Gruppo: **ciascuna funzione aziendale, chiamata ad avviare una nuova attività che possa comportare il trattamento di dati personali o a gestire trattamenti preesistenti con nuove modalità, deve contattare preventivamente il DPO per tutti gli approfondimenti e le verifiche sugli aspetti di compliance (normativa, di analisi del rischio e di sicurezza).**

Il tool informatico utilizzato dal Gruppo LAVAZZA per mappare i trattamenti dei dati consente di valutare i possibili rischi derivanti dalla progettazione di un nuovo trattamento e di procedere eventualmente ad una valutazione d'impatto sulla protezione dei dati (DPIA) al fine di apportare i dovuti correttivi (cfr. paragrafo 9).

9. Valutazione di impatto sulla protezione dei dati (DPIA)

Quando un tipo di trattamento, in particolare se prevede l'utilizzo di nuove tecnologie o se risulta essere di nuova applicazione, presenta un **rischio elevato** per i diritti e le libertà degli Interessati, le Società del Gruppo **prima di procedere al trattamento stesso** – effettuano una **valutazione di impatto sulla protezione dei dati personali**, volto a determinare in particolare la probabilità e la gravità di tale rischio tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.

L'esito della valutazione dev'essere preso in considerazione nella determinazione delle opportune misure e garanzie da adottarsi per l'attenuazione del rischio e per il rispetto delle disposizioni di cui al Regolamento.

Qualora tali misure non siano adottabili, in considerazione delle tecnologie disponibili o dei costi di attuazione, occorre consultare l'autorità di controllo prima dell'inizio delle attività di trattamento.

La valutazione di impatto dev'essere aggiornata, con l'assistenza del DPO e il supporto dei Referenti Interni, periodicamente o comunque ogni qual volta si riveli necessario alla luce del tempo trascorso dal trattamento iniziale o vi siano cambiamenti significativi nel trattamento nella tipologia dei dati trattati, nelle modalità di trattamento, nelle soluzioni tecnologiche impiegate che possono aver modificato significativamente le analisi iniziali.

La valutazione prende in considerazione l'intero "ciclo di vita" dei dati personali, dalla raccolta alla cancellazione e tiene conto di eventuali elementi specifici richiesti dal particolare contesto nel quale avvengono i trattamenti (es. marketing diretto, profilazione, dati dei minori, ecc.) nonché della normativa applicabile.

La valutazione d'impatto è, comunque, obbligatoriamente eseguita nei seguenti casi:

- trattamento automatizzato, compresa la profilazione, sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente sugli Interessati;
- il trattamento, su larga scala¹⁵, di categorie particolari di dati personali che presentano un elevato rischio per i diritti e le libertà degli Interessati;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

10. Valutazione di impatto sul trasferimento dei dati (TIA)

Quando i dati personali trattati devono essere trasferiti verso Società del Gruppo o verso Terze Parti ubicate in Paesi al di fuori dell'UE/SEE che non offrono un adeguato livello di protezione ovvero una protezione equivalente a quella fornita dal Gdpr, prima di procedere al trattamento, occorre effettuare una valutazione di impatto sul trasferimento dei dati personali ("Transfer Impact Assessment" o "TIA") volta a valutare la normativa vigente nel Paese di trasferimento ed i rischi e la gravità degli stessi per i diritti e le libertà dei soggetti interessati, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.

Le Società del Gruppo interessate dalla necessità di predisporre la TIA sono tenute a documentare il processo di valutazione d'impatto del trasferimento e, ove richiesto, di metterla a disposizione dell'Autorità di controllo competente.

L'esito della valutazione dovrà essere preso in considerazione nella determinazione delle **ulteriori misure** e garanzie da adottarsi per l'attenuazione del rischio e per il rispetto delle disposizioni di cui al Regolamento.

11. Notifica in caso di violazione dei dati personali

Una violazione di dati personali (**Data Breach**) può, se non affrontata in modo adeguato e tempestivo, provocare danni nei confronti degli Interessati, quali: perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti; discriminazione, furto o usurpazione di identità; perdite finanziarie; pregiudizio alla reputazione; perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Pertanto, nei casi di violazione dei dati personali, la Società del Gruppo LAVAZZA che ha subito la violazione deve:

- verificare che siano state messe in atto tutte le misure tecnologiche ed organizzative adeguate di protezione in funzione della violazione;
- informare tempestivamente e comunque non oltre le 24 ore il Titolare del trattamento, il Delegato (ove nominato) e il DPO locale e di Gruppo ai fini della notifica dell'evento all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne viene a conoscenza.

¹⁵ I trattamenti su larga scala mirano al trattamento di una notevole quantità di dati personali che, potendo incidere su un vasto numero di Interessati, potenzialmente possono presentare un rischio elevato per i diritti e le libertà degli Interessati.

Il Gruppo Lavazza ha provveduto a definire ed emanare, con il supporto del DPO, la Procedura di Data Breach per una corretta gestione degli incidenti di sicurezza relativi ai dati personali che si richiama integralmente per quanto riguarda le modalità operative previste dalla procedura medesima.

A titolo esemplificativo e non esaustivo, gli eventi di possibile violazione dei dati personali possono essere costituiti da:

- **perdita irrimediabile di dati (siano essi in formato elettronico o cartaceo)** intesa come accertata impossibilità di ripristino degli stessi. A titolo di esempio: casi di smarrimento/furto di supporti informatici o eventi di incendio/allagamento di archivi cartacei;
- **accesso non autorizzato ai dati (sistemi informatici o archivi cartacei)** inteso come violazione della confidenzialità dei dati contenuti negli stessi sistemi o archivi. A titolo di esempio: un attacco informatico tramite lo sfruttamento di vulnerabilità dei sistemi o l'uso abusivo di credenziali di autenticazione; la consultazione di archivi cartacei il cui accesso è definito ristretto al solo personale autorizzato;
- **perdita dell'integrità dei dati** intesa come compromissione irrimediabile della correttezza, congruenza e consistenza dei dati. A titolo di esempio: compromissione derivante da modifica non autorizzata dei dati, da errore umano, da incidenti di natura informatica;
- **rivelazione o divulgazione di dati (siano essi in formato elettronico o cartaceo) a soggetti terzi non legittimati**, anche non identificati, ad esempio tramite la posta elettronica o anche verbalmente.

Appena nota, ogni situazione di violazione di dati personali dovrà essere tempestivamente segnalata da chi ne è venuto a conoscenza:

- per la LUIGI LAVAZZA S.p.A., al proprio Referente Interno, al DPO, al IT Governance & Security Manager nell'ambito della funzione ICT e al Service Desk Centralizzato, nonché alla Funzione Corporate Affairs & Compliance;
- per tutte le altre Consociate, al proprio Focal Point Privacy, al Referente Interno e al Service Desk Centralizzato; sarà cura del Focal Point e del Referente Interno informare tempestivamente e comunque non oltre le 24 ore, il DPO locale e di Gruppo, l'IT Governance & Security Manager nell'ambito della funzione ICT di HQ e la Funzione Corporate Affairs & Compliance HQ.

Una volta ricevuta la segnalazione, il DPO informerà immediatamente il Titolare del Trattamento e, con il supporto del Comitato Privacy, procederà alla valutazione della anomalia.

Solo nel caso in cui l'evento venga effettivamente ritenuto un Data Breach, il Titolare del Trattamento prenderà atto dei mezzi correttivi necessari (attività di mitigazione del Data Breach) e, a meno che risulti improbabile che la violazione presenti un rischio per i diritti e le libertà degli Interessati, notificherà la violazione accertata all'autorità di controllo competente, **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**.

Nel caso in cui la violazione esponga gli Interessati a **rischi elevati**, il Titolare invierà, senza indebito ritardo, una comunicazione diretta a ciascuno degli stessi, descrivendo la natura della violazione accertata.

12. Ispezioni dell'Autorità di controllo

Le autorità di controllo competenti possono effettuare ispezioni presso le Società del Gruppo LAVAZZA finalizzate a verificare l'effettiva applicazione da parte di queste ultime delle disposizioni di legge.

Nel corso di tali ispezioni, il Gruppo adotterà le cautele ed i presidi previsti dalla regolamentazione interna riguardante i rapporti con le Autorità di pubblica vigilanza.

In generale, a fronte di contatti con funzionari rappresentanti gli uffici dell’Autorità di controllo, occorre immediatamente avvisare il proprio Referente Interno e il DPO.

Documenti o informazioni connesse al trattamento di dati personali possono essere consegnati agli ispettori solo con autorizzazione di un rappresentante della Direzione Affari Legali della Capogruppo, che dovrà assistere alla visita ispettiva.

Il DPO di Gruppo o locale, ove presente, con il supporto della Funzione Corporate & Compliance della Capogruppo LUIGI LAVAZZA S.p.A., è incaricato di fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, facilitando l’accesso dell’Autorità alle informazioni necessarie e cooperando con la medesima.

12.1 Regole comportamentali in caso di attività ispettive

Tutto il personale, a qualsiasi titolo coinvolto nella gestione di visite ispettive dell’Autorità di Controllo, è tenuto ad osservare le norme comportamentali indicate dalla Società presso la quale presta la propria attività lavorativa, nonché le Policy e le procedure in materia.

Si richiamano integralmente le modalità operative previste dalla procedura di Gestione delle Visite Ispettive (PR_LL_L1).

In linea generale, si raccomanda di assumere un atteggiamento collaborativo con l’Autorità di controllo: il dovere di collaborazione implica l’obbligo di consentire l’accesso ai documenti, sia cartacei che in formato elettronico contenuti in computer, hard disk nonché in ogni altro dispositivo informatico, l’obbligo di indicare dove sono conservati i documenti d’interesse nonché l’obbligo di fornire ogni informazione richiesta indipendentemente dal fatto che i documenti o le informazioni siano tenute in luoghi diversi o da soggetti diversi dalle Società del Gruppo, Titolari o Responsabili del trattamento, (quali Terze parti Responsabili del trattamento).

Le risposte ai quesiti formulati dagli ispettori devono fare riferimento il più possibile alle procedure adottate ed ai trattamenti di dati personali effettuati, in modo da evitare risposte generiche, riservandosi – in caso di incertezza - di fornire, anche successivamente, chiarimenti e/o risposte nonché documentazione più dettagliata.


13. Formazione

Il piano di formazione in materia privacy (corsi, destinatari, tempi) è definito, a livello di Gruppo, su impulso del Titolare del trattamento, dalle Funzioni HR e Corporate Affairs & Compliance della Capogruppo in coordinamento con il DPO e il Comitato Privacy.

La formazione si prefigge l’obiettivo di formare ed informare i Referenti Interni ed i soggetti autorizzati al trattamento riguardo a:

- ambiti legislativi, adeguamento alla normativa ed ai Provvedimenti del Garante Privacy;
- tipologia di dati e modalità di trattamento degli stessi;
- modello di gestione della Privacy implementato;
- ruoli previsti per il trattamento dei dati personali;
- informativa e consenso, diritti di accesso, reclami e sanzioni;
- le misure di sicurezza adottate.

Nei casi di nuove assunzioni, cambio mansione o introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento di dati personali, la Funzione HR – con il supporto del Comitato Privacy - ha la responsabilità di prevedere che il piano formativo venga aggiornato ed erogato in tempi ragionevolmente brevi.

A decorative graphic in the top left corner consisting of several coffee beans and a yellow circle, with thin yellow lines extending from them.

Il Gruppo LAVAZZA mette a disposizione l'erogazione di una formazione *on line*, da erogarsi sul portale della formazione a tutti i dipendenti in possesso di supporto informatico (pc o telefono cellulare), ed una formazione in aula per i Referenti Interni di primo livello (primi riporti dell'AD e dei GM).

14. Audit

La Funzione Internal Audit di Gruppo, nell'ambito delle attività previste dal piano di Audit, può svolgere attività di *assurance* sul livello di conformità alle regole previste dal presente documento e al quadro normativo di riferimento, partendo dalle risultanze delle eventuali verifiche condotte dal DPO o da soggetti espressamente incaricati, riservandosi, all'occorrenza, di effettuare approfondimenti e/o ulteriori verifiche ad hoc.

Le attività di audit possono essere estese anche a Terze Parti (fornitori) che operano in nome e per conto delle singole società del Gruppo.

15. Sanzioni

La violazione della normativa in materia di protezione dei dati personali può esporre le Società del Gruppo a diverse tipologie di responsabilità e conseguenti sanzioni (di carattere amministrativo e/o penale) a seconda delle norme concretamente violate ed avere sul Gruppo LAVAZZA significativi impatti reputazionali negativi, anche rilevanti.

L'inosservanza degli obblighi previsti dalla presente Policy costituisce comportamento rilevante ai fini disciplinari e può determinare l'applicazione delle sanzioni disciplinari previste dalle leggi vigenti e dai contratti di lavoro nazionali.