MODELLO
PER L'ATTUAZIONE ED IL RISPETTO DELLE DISPOSIZIONI DI CUI AL REGOLAMENTO UE 679/2016
LABCAM SRL

Edizione	1	2	3	4	5
Emissione	12.11.2021				
Approvato Direttore	17.11.2021				

INDICE

§ 1. INTRODUZIONE

In data 27 aprile 2016 è stato emanato il Regolamento UE n.679/2016, le cui disposizioni si applicano a fare data dal 25 maggio 2018, denominato Regolamento Generale sulla Protezione dei Dati (di seguito denominato "*il Regolamento*"). Tale Regolamento è stato introdotto al fine di armonizzare compiutamente tutte le normative europee in tema di privacy e di adeguarle alle esigenze sorte con il progresso tecnologico.

Il Regolamento, di immediata applicazione nel nostro paese, integra la previgente disciplina relativa al trattamento dei dati personali (D.lgs 196/2003 e ss. modifiche ed integrazioni).

Scopo del presente modello organizzativo è la ricognizione delle idonee misure giuridiche tecniche ed organizzative, già prima d'ora predisposte ed attuate, da parte dell'impresa, al fine di garantire l'attuazione ed il rispetto delle disposizioni e dei principi introdotti dal Regolamento e dalla previgente normativa, prevedendo, altresì, continui processi di monitoraggio e di adeguamento alle norme di legge. Il presente documento comprova, quindi, l'attività posta in essere da Labcam e che ha consentito alla stessa di porre in essere le azioni per adeguarsi alle disposizioni del Regolamento UE 2016/679, ai contenuti del testo del decreto privacy attuativo del GDPR pubblicato in Gazzetta Ufficiale del 4 settembre 2018 ed alle successive indicazioni del Garante.

Occorre altresì, preliminarmente, dare conto della circostanza che Labcam ha provveduto, con atto di designazione del 29.06.2021, alla **nomina del DPO e/o Responsabile Trattamento Dati**, il quale ha avvallato il presente Modello e le misure organizzative ivi previste, supportando i referenti aziendali nella redazione del documento.

Sul sito web istituzionale (https://www.labcam.it/site/wp-content/uploads/CCF29062021.pdf) è pubblicato l'atto di nomina, comunicato al Garante ed è presente una sezione Internet Privacy Policy, ove è **pubblicato il presente Modello (Parte Generale)**, nonché una sintesi concernente le seguenti informazioni:

1- Titolare del trattamento (riferimenti e recapiti)

2- DPO: riferimenti ed indirizzo di contatto

3- Finalità e base giuridica del trattamento: indicazione di sintesi in merito alle finalità per le quali Labcam effettua il trattamento di dati personali nei limiti di quanto ciò sia strettamente necessario allo svolgimento della propria attività

4- Modalità di trattamento

5- Dati di navigazione: informativa in merito ai sistemi informatici e alle procedure software preposte al funzionamento del sito web ed alla presenza di Cookies

6- Destinatari dei dati: informativa in merito agli eventuali soggetti destinatari dei dati

7- Conservazione dei dati: informativa circa il periodo di conservazione dei dati personali, differenziato a seconda del campo di applicazione, ma in ogni caso stabilito per un arco di tempo non superiore al conseguimento delle finalità, o fino alla richiesta di cancellazione, per le quali sono raccolti e trattati

8- Diritti dell'interessato e forme di tutela.

§ 2. ATTIVITÀ DI PREDISPOSIZIONE DEL MODELLO

L'attività si è estrinsecata in una analisi preliminare del contesto aziendale, al fine di avere un quadro completo e schematizzare l'organizzazione dei ruoli, dei processi e delle regole di gestione dei dati, i flussi informativi tra

i vari uffici e verso l'esterno, la documentazione che ha effetti sul trattamento, le tecnologie e gli strumenti per la gestione della sicurezza informatica (logica) e fisica, i sistemi di controllo interno.

La precitata analisi si è pertanto svolta, coerentemente con quanto sopra esposto, tramite una ricognizione, coinvolgendo i vari "referenti", al fine di verificare la tipologia di dati trattati, la finalità del trattamento, le tecnologie utilizzate ed i flussi dei dati medesimi.

§ 3. CORE BUSINESS ED ATTIVITÀ DI LABCAM

Il Laboratorio Chimico Merceologico della Camera di Commercio di Savona ha iniziato la propria attività nel 1995 grazie alla sua realizzazione voluta dalla Camera di Commercio Industria Agricoltura ed Artigianato di Savona d'intesa con tutti i settori produttivi della provincia. Storicamente i Laboratori delle Camere di Commercio, nati in Italia a partire dall'inizio del secolo scorso, forniscono servizi di certificazione pubblica garantendo una funzione fortemente imparziale, suddividendo il loro impegno tra compiti istituzionali e servizi alle imprese e al privato cittadino, svolgendo anche funzioni di assistenza alle imprese per il miglioramento qualitativo dei prodotti e dei processi produttivi, per aiutarle ad adeguarsi alle specifiche di legge e alla normativa volontaria. L'attività che il Laboratorio offre alla platea degli utilizzatori, principalmente imprese di produzione e di distribuzione, istituzioni pubbliche e private, associazioni di categoria e privati cittadini, riguarda una vasta gamma di analisi chimiche, microbiologiche e sensoriali. Queste prestazioni possono essere erogate a livello nazionale, anche avvalendosi di specifiche, qualificate e riconosciute competenze territoriali. Attraverso i propri servizi di analisi, eseguiti da personale specializzato con strumenti ed attrezzature all'avanguardia, il Laboratorio Chimico Merceologico è in grado di rispondere a qualsiasi esigenza analitica e di ricerca nei settori: - agroalimentari (aspetti nutrizionali, micotossine, additivi, allergeni, metalli pesanti, valutazioni organolettiche, determinazioni ufficiali nel settore vitivinicolo e oleico); - industriali (centro di saggio, controllo qualità e di produzione); - ambientali (acque superficiali, sotterranee, potabili e reflue, classificazione dei rifiuti, inquinanti aereodispersi, ambienti di lavoro); - agronomiche (terreni, acque irrigue, soluzioni nutritive di fertirrigazione impiegate in agricoltura); - microbiologiche (acque potabili, irrigue e reflue, alimenti per prove di conformità ai requisiti igienico sanitari e dell'efficacia di autocontrollo e HACCP, Legionella, ambienti e superfici di lavoro).

Il Laboratorio Chimico Merceologico è inoltre un Centro di Saggio Residui riconosciuto dal Ministero della Salute in conformità alla Buona Pratica di Laboratorio (BPL) secondo D.Lgs n° 50 del 02/03/2007 – Dir. 2004/09/CE. Il Centro di Saggio Residui è l'unico riconosciuto in Liguria e garantisce un supporto all'industria nazionale ed internazionale per la verifica di residui chimici richieste dalla normativa in vigore e dal Ministero della Salute.

Nel polo tecnologico della Camera di Commercio Industria Artigianato ed Agricoltura di Savona sono state realizzate, conformemente a quanto previsto dai regolamenti e dagli standard normativi internazionali, due sale di assaggio per la valutazione organolettica di vino e olio. Le valutazioni organolettiche, soprattutto negli ultimi anni, hanno assunto un'importanza sempre maggiore diventando a tutti gli effetti prove oggettive di classificazione merceologica degli alimenti. Le prove sono eseguite da un gruppo di persone (in inglese "Panel") che esprimono il loro giudizio secondo norme e procedure standardizzate per evidenziare attributi positivi o negativi (difetti). Le analisi organolettiche eseguite presso il Polo di Albenga sono indirizzate verso molteplici alimenti, spaziano dai prodotti vegetali alle matrici complesse, frutto di lavorazioni più o meno elaborate. In alcuni casi sono anche indirizziate verso la classificazione in riferimento a parametri previsti dai disciplinari di origine DOP, come ad esempio per gli oli di oliva, e IGT come ad esempio per la pasta. Nel caso degli olii il Laboratorio Chimico Merceologico ha un Panel professionale di assaggio riconosciuto dal Ministero delle Politiche Agricole e Forestali ed è una delle pochissime strutture in Italia accreditate da ACCREDIA in conformità alla norma UNI CEI EN ISO/IEC 17025:2005 proprio per tale prova di assaggio. Nel caso del caffè, è invece

l'unico in Italia ad avere questo riconoscimento, avendo accreditato il "CUP TEST all'italiana", solo modo per qualificare il caffè tostato ed estratto anche come espresso. Infatti, il cup test alla brasiliana, metodo che normalmente accompagna i caffè verdi, dà informazioni sulla presenza/assenza di difetti, ma nulla dice sulle caratteristiche organolettiche del prodotto qualora venga lavorato per un'estrazione da consumatore, sia essa per moka, espresso, infusione o percolazione. Essendo la prova accreditata, le valutazioni espresse sono riconosciute come oggettive e, quindi, i Rapporti di Prova hanno valenza inconfutabile nei Paesi aderenti all'ISO (organizzazione internazionale per la normazione) e rappresentano un potente veicolo anche per la diffusione dell'espresso italiano nel mondo. Il contributo di esperti sul caffè internazionalmente riconosciuti, che operano sia presso la nostra sede che in sedi periferiche, fa sì che il Polo di Albenga costituisca ora un centro di eccellenza anche sull'analisi del caffè. Questa competenza pluridecennale è a supporto di tutti gli operatori del settore, sia nazionale che estero, sia dal punto di vista analitico che culturale. La sezione relativa alle analisi sensoriali si appoggia sia su dipendenti del Laboratorio in formazione continua che su alcuni assaggiatori iscritti agli Albi della Regione Liguria, che operano mediante prestazioni occasionali. Il Laboratorio Chimico Merceologico ha inoltre, nell'oggetto della certificazione UNI EN ISO 9001, i servizi relativi alle "Analisi sensoriali su alimenti". La specializzazione nella attività è stata estesa alle conserve alimentari in genere ed in particolare a due alimenti della nostra tradizione regionale: le olive da mensa e il pesto.

Nel caso delle olive da mensa il panel del Laboratorio partecipa a circuiti di controlli internazionali gestiti dal Consiglio Oleicolo Internazionale (COI) che ha sede a Madrid ed è l'unico Panel al mondo Accreditato per la norma COI COI/OT/MO/N° 1 per la valutazione organolettica dell'oliva da mensa. In molti casi l'analisi organolettica, come visto per l'olio di oliva, affianca le classiche prove chimiche e microbiologiche qualora si voglia verificare la genuinità e la stabilità dei prodotti nel tempo. Questo permette alle aziende di commercializzare alimenti conformi a quanto previsto dalla normativa vigente e nello stesso tempo di soddisfare le esigenze di gradimento del consumatore finale. L'abbinamento della ricerca sensoriale alle classiche tecniche d'indagini chimiche, ad esempio per la valutazione dei profili aromatici degli alimenti, possono essere realizzati direttamente nella struttura sfruttando la possibilità di utilizzare un unico centro altamente specializzato in entrambe le scienze applicate.

Il Laboratorio, oltre a realizzare analisi e prove sui prodotti, effettua anche servizi di assistenza in alcuni ambiti strategici, come: - interpretazione dei risultati analitici, implementazione di sistemi di monitoraggio ambientale - controllo dei punti critici dei processi del settore alimentare (HACCP) - etichettatura dei prodotti, certificazioni per l'export etc; - implementazione di Sistemi di Gestione - elaborazione di Disciplinari di Prodotto - audit di parte seconda - formazione.

In merito alle attività di erogazione di servizi formativi, la Società propone da anni dei corsi su varie tematiche ed offre percorsi mirati su specifiche richieste. In quest'ottica l'attività della struttura è stata improntata secondo un sistema di gestione qualità certificato sia UNI EN ISO 9001:2008 che UNI CEI EN ISO/IEC 17025:2005 al fine di garantire sia il processo di analisi in generale (dal campionamento all'emissione del rapporto di prova) sia in particolare l'attendibilità delle prove stesse. Allo scopo, sono state appositamente dedicate delle figure professionali, specifiche per ogni settore d'interesse alle aziende, uno specialista del settore è infatti dedicato all'assistenza e alla trasmissione delle informazioni necessarie per la risoluzione di eventuali problemi emersi nella realtà quotidiana.

Del pari occorre ricordare la circostanza che la Società è dotata di numerose certificazioni / accreditamenti, i quali comprovano il costante perseguimento di obiettivi di buona gestione societaria.

§ 4. ORGANIGRAMMA, RUOLI E RESPONSABILITÀ

Gli Organi sociali risultano così composti.

Ai sensi dello Statuto Labcam è amministrata da un **Consiglio di Amministrazione** composto da tre a cinque membri, compreso il Presidente nominato, previa deliberazione dell'Assemblea ordinaria, in conformità alle vigenti disposizioni in materia di società controllate da pubbliche amministrazioni e di parità di accesso agli organi di amministrazione e di controllo (art.10). I componenti del Consiglio di Amministrazione devono essere scelti tra persone particolarmente qualificate nelle attività economiche e professionali connesse all'oggetto sociale. Durano in carica per il periodo di tempo stabilito dai Soci e scadono alla data dell'assemblea convocata per l'approvazione del bilancio relativo all'ultimo esercizio della loro carica, e sono rieleggibili (art.11).

Il **Sindaco** di Labcam, con funzioni di Revisore Unico, è investito delle funzioni previste dall'art. 2403 e 203 bis c.c..

La definizione dei ruoli e delle responsabilità è il primo passo da compiere al fine della compliance al GDPR. Di seguito sono riepilogati compiti e responsabilità delle diverse figure presenti in Labcam con riferimento alla normativa "privacy", sia che questi derivino da un incarico specifico come nel caso del DPO, sia che siano collegati a posizioni gerarchicamente rilevanti.

DIRETTORE GENERALE. Ai sensi del vigente Statuto (art.13) particolare rilievo assume la figura del Direttore Generale, poiché lo stesso competono specifici poteri ed attribuzioni –tanto di natura ordinaria che straordinaria- nella conduzione della società in materia di sicurezza, ambiente, organizzazione e gestione del personale, approvvigionamenti, forniture e clientela. In particolare il Direttore concorre nella attuazione dei programmi e cura l'esecuzione delle delibere del CDA ed elabora insieme al Consiglio le linee guida strategiche, il business plan ed il budget annuale della Società.

REFERENTI DI AREA

Ai Referenti sono delegate le seguenti funzioni:

a) applicano - nel contesto della specifica *mission* dell'Area di riferimento - la normativa e le procedure/istruzioni/indicazioni in materia di protezione dei dati personali definite dal Titolare in collaborazione con il RPD; i Referenti sono destinatari di ogni comunicazione concernente l'adozione da parte della Società di atti di carattere generale (ad es., regolamenti, procedure, circolari, linee guida, provvedimenti...) in materia di privacy e ne garantiscono l'applicazione;

b) verificano le esigenze di integrazione od aggiornamento dei documenti gestionali predisposti, ad es., evidenziando a RPD le eventuali necessità di modifica/integrazione del registro dei trattamenti di cui all'art.30 del Regolamento, in relazione, ad esempio, a:

- esigenze derivanti da nuovi servizi/progetti diversi o nuovi rispetto a quelli attualmente censiti;

- modifiche organizzative interne all'Area di competenza che comportino diverse modalità di gestione dei trattamenti di dati, anche ai fini dell'analisi dei rischi;

c) adottano ordinariamente, ovvero in caso di criticità e problematiche sopravvenute, tutte le misure preventive e correttive a tutela dei dati personali che le competenze connesse al ruolo consentano di assumere (rientranti nell'ambito delle funzioni), rappresentando ad RPD specifiche esigenze cui non possono far fronte ordinariamente;

d) garantiscono, in relazione alle necessità di volta in volta emergenti nell'ambito dei servizi di competenza, il rilascio dell'informativa di cui agli artt. 13 e 14 del GDPR e l'acquisizione del consenso dagli interessati (ove necessario);

e) garantiscono che la diffusione dei dati personali (diversi da quelli sensibili e giudiziari che risulta allo stato essere vietata) avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero solo se prevista da specifica normativa (ad es., con riferimento agli obblighi di pubblicazione per finalità di pubblicità integrativa dell'efficacia e di trasparenza (ai sensi del D.Lgs. 33/2013 e s.m.i.) per quanto di competenza;

f) si attivano - in collaborazione con il RPD - per fare in modo che, in relazione ad ogni nuova iniziativa o progetto che comporti un trattamento di dati personali, sia effettuata una verifica preventiva della liceità e della legittimità del trattamento, nonché delle modalità con le quali si intende eseguirlo; ove necessario, sulla base degli artt. 35 e 36 del Regolamento e delle Linee guida WP29 e del Garante, provvedono ad eseguire, in collaborazione con RPD, la valutazione d'impatto sulla protezione dei dati e supportare il Presidente nell'attivazione della consultazione preventiva del Garante ove ritenuta necessaria;

g) gestiscono i flussi informativi al RPD di propria competenza, come definiti nell'apposito paragrafo del presente documento, e più in generale comunicano allo stesso di ogni notizia rilevante ai fini della protezione dei dati personali e degli interessati.

SOGGETTI INCARICATI

Il personale autorizzato deve effettuare le operazioni di trattamento secondo le istruzioni impartite dai soggetti di cui ai paragrafi precedenti, e rimane soggetto al potere di vigilanza e controllo di questi ultimi. In particolare, i soggetti autorizzati dovranno:

a) garantire la massima riservatezza su qualsiasi informazione e dato personale di cui vengano a conoscenza nell'esercizio delle proprie funzioni, in conformità a quanto previsto normativamente in tema di segreto d'ufficio e di segreto d'impresa;
b) fare riferimento al registro dei trattamenti per l'individuazione degli elementi fondamentali dei trattamenti che si è autorizzati ad effettuare;
c) seguire obbligatoriamente i percorsi formativi che saranno organizzati dalla Società;
d) rispettare le disposizioni impartite con riferimento alla materia in oggetto;
e) comunicare al diretto responsabile, al Direttore o anche direttamente al RPD, ogni notizia rilevante ai fini della protezione dei dati personali e degli interessati; collaborare più in generale con il RPD provvedendo a fornire ogni informazione da questi richiesta.

Il soggetto autorizzato potrà fare riferimento direttamente a RPD per l'esercizio dei diritti che gli sono propri in qualità di interessato al trattamento dei propri dati personali (artt. 15 e ss. del GDPR).

RESPONSABILE PROTEZIONE DATI

Il RPD (o DPO) costituisce una figura di riferimento per tutte le questioni di carattere generale riguardanti la protezione dei dati personali. In particolare, all'RPD sono affidati i seguenti compiti:

- supportare il Titolare del trattamento nel percorso di implementazione del GDPR a livello organizzativo-gestionale e tecnico-informatico, esprimendo pareri sui documenti di carattere gestionale e sulle soluzioni tecnico-informatiche che vengono progettate per la *compliance* generale della Società;

- informare e consigliare il Titolare del trattamento ed i dipendenti sugli obblighi derivanti dal GDPR e dalla normativa nazionale; in questo ambito, all'RPD potrà essere richiesto di partecipare ad incontri operativi ai vari livelli in cui vengano assunte decisioni relative al trattamento dei dati personali;

- sorvegliare l'osservanza del GDPR e delle politiche interne in materia di protezione dei dati, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale, anche attraverso l'analisi degli esiti di audit e visite ispettive programmati e/o a sorpresa;

- fornire, se richiesto, pareri sulla valutazione d'impatto del trattamento sulla protezione dei dati di cui agli artt. 35 e ss. del Regolamento, in particolare: sorvegliandone lo svolgimento, provvedendo ad esaminarne gli esiti finali e supportando le decisioni connesse agli obblighi di consultazione preventiva del Garante;

- partecipare alle istruttorie e valutazioni circa eventuali violazioni di dati personali occorsi presso Labcam, supportando il Titolare nelle decisioni circa la gestione delle notificazioni dei data breach di cui agli artt. 33 e 34 del GDPR secondo quanto previsto nell'apposita procedura gestionale;

- con riferimento al punto precedente, provvedere alla alimentazione ed aggiornamento del "Registro dei data breach";

- cooperare con il Garante italiano e con quello di eventuali paesi esteri con cui Labcam dovesse entrare in contatto, e fungere da punto di riferimento per facilitare l'accesso, da parte di questa, ai documenti ed alle informazioni necessarie ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi alla stessa attribuite dal GDPR;

- fungere da punto di contatto e curare i rapporti con gli interessati, coinvolgendo i referenti competenti *ratione materiae* nell'analisi ed evasione di ogni questione che venga sottoposta direttamente alla propria attenzione ovvero all'attenzione del Titolare del trattamento; in proposito si specifica che, pur nel caso in cui la richiesta di esercizio dei diritti sia sottoposta al RPD, la decisione sul riconoscimento o meno del diritto – e la relativa comunicazione all'interessato – spetta esclusivamente al Titolare;

- con riferimento al punto precedente, provvedere alla istituzione, alimentazione ed aggiornamento del "Registro delle richieste di esercizio dei diritti degli interessati";

- formalizzare, se richiesto, relazioni al Titolare del trattamento in merito alle attività di supporto interno e di controllo effettuate, all'implementazione delle misure suggerite, o valutazioni generali e specifiche sulla *compliance* di Labcam al GDPR.

L'ambito d'intervento del RPD comprende tutti i trattamenti di dati personali posti in essere da Labcam, compresa l'attività eventualmente delegata a soggetti esterni (persone fisiche e giuridiche), nonché quelli per i quali la Azienda è stata nominata responsabile ex art. 28.

Per l'RPD sono previsti requisiti di autonomia ed indipendenza nell'esecuzione dell'incarico, infatti allo stesso sono attribuiti i seguenti poteri e prerogative:

a) potere di autoregolamentazione. Il RPD può programmare autonomamente le proprie attività, garantendo comunque l'assolvimento dei compiti precedentemente indicati e rendendo conto delle attività effettivamente espletate ai fini della verifica di idoneità ed efficace attuazione sistema privacy implementato rispetto agli obblighi di cui al GDPR; il RPD può farsi coadiuvare da personale appartenente alla propria Struttura organizzativa dotato di competenze specifiche nella materia, ferma restando la responsabilità finale dello stesso sugli atti ed indicazioni formalizzate;

b) poteri ispettivi: nell'esercizio delle proprie funzioni di controllo, il RPD può:

- utilizzare le risultanze di attività ispettive interne ovvero svolgere autonomamente verifiche anche a sorpresa;
- accedere liberamente ad ogni documento rilevante per lo svolgimento delle sue funzioni;
- disporre l'acquisizione di informazioni, dati e/o notizie a semplice richiesta, senza preventiva autorizzazione;
- richiedere l'audizione ovvero il coinvolgimento nelle attività di verifica di qualsivoglia dipendente dell'Ente;

Nell'esercizio dell'incarico, il RPD garantisce il vincolo di riservatezza sui dati e sulle informazioni acquisite, fermi restando gli obblighi connessi ad eventuali richieste formalizzate da Pubbliche autorità con funzioni inquirenti, giudicanti e di controllo.

I dati di contatto del RPD (recapito postale, telefono, email), comunicati al Garante per la protezione dei dati personali, sono resi disponibili, sul sito internet istituzionale e riportati nelle informative rese agli interessati.

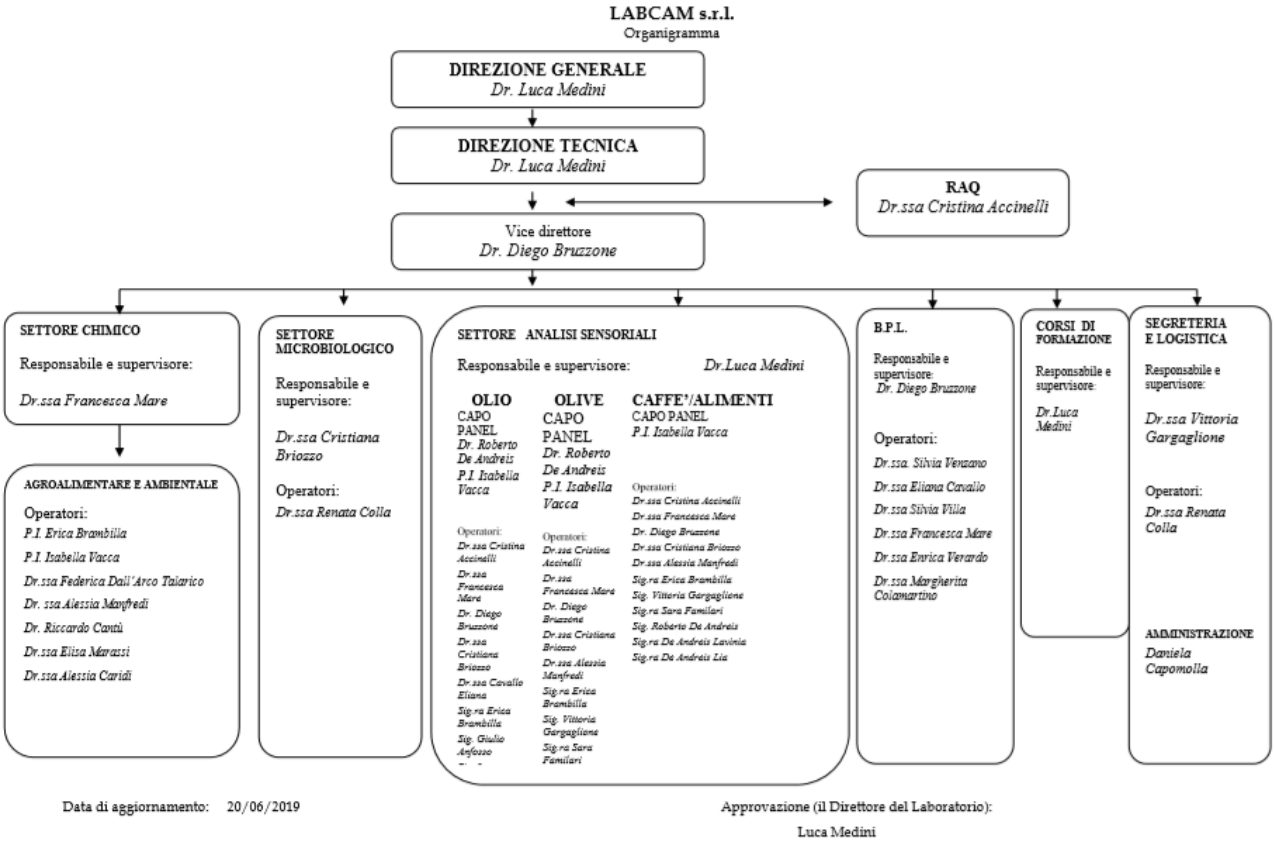
RESPONSABILE PER LA PREVENZIONE DELLA CORRUZIONE E LA TRASPARENZA (RPCT)

A seguito del Reg UE 2016/679, recepito da ANAC in sede di PNA 2018 occorre "*ricordare che le pubbliche amministrazioni, prima di mettere a disposizione sui propri siti web istituzionali dati e documenti (in forma integrale o per estratto, ivi compresi gli allegati) contenenti dati personali, verifichino che la disciplina in materia di trasparenza contenuta nel d.lgs. 33/2013 o in altre normative, anche di settore, preveda l'obbligo di pubblicazione. Giova rammentare, tuttavia, che l'attività di pubblicazione dei dati sui siti web per finalità di trasparenza, anche se effettuata in presenza di idoneo presupposto normativo, deve avvenire nel rispetto di tutti i principi applicabili al trattamento dei dati personali contenuti all'art. 5 del Regolamento (UE) 2016/679. In particolare assumono rilievo i principi di adeguatezza, pertinenza e limitazione a quanto necessario rispetto alle finalità per le quali i dati personali sono trattati («minimizzazione dei dati») (par. 1, lett. c) e quelli di esattezza e aggiornamento dei dati, con il conseguente dovere di adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (par. 1, lett. d) 8. Il medesimo d.lgs. 33/2013 all'art. 7 bis, co. 4, dispone inoltre che «Nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le pubbliche amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione». Si richiama anche quanto previsto all'art. 6 del d.lgs. 33/2013 rubricato "Qualità delle informazioni" che risponde alla esigenza di assicurare esattezza, completezza, aggiornamento e adeguatezza dei dati pubblicati. Al riguardo, si rinvia alle più specifiche indicazioni fornite dal Garante per la protezione dei dati personali. Si ricorda inoltre che, in ogni caso, ai sensi della normativa europea, il Responsabile della Protezione dei Dati-RPD (vedi infra paragrafo successivo) svolge specifici compiti, anche di supporto, per tutta l'amministrazione essendo chiamato a informare, fornire consulenza e sorvegliare in relazione al rispetto degli obblighi derivanti della normativa in materia di protezione dei dati personali (art. 39 del RGPD)*"

Relativamente ai rapporti tra RPCT e Responsabile della Protezione dei Dati -RPD-, un indirizzo interpretativo è stato sollecitato all'Autorità da diverse amministrazioni. Ciò in ragione della circostanza che molte amministrazioni e soggetti privati tenuti al rispetto delle disposizioni contenute nella l. 190/2012, e quindi alla nomina del RPCT, sono chiamate a individuare anche il RPD. Come chiarito dal Garante per la protezione dei dati personali l'obbligo investe, infatti, tutti i soggetti pubblici, ad esempio, le amministrazioni dello Stato, anche

con ordinamento autonomo, gli enti pubblici non economici nazionali, regionali e locali, le Regioni e gli enti locali, le università, le Camere di commercio, industria, artigianato e agricoltura, le aziende del Servizio sanitario nazionale, le autorità indipendenti ecc. Secondo le previsioni normative, il RPCT è scelto fra personale interno alle amministrazioni o enti (si rinvia al riguardo all'art. 1, co. 7, della l. 190/2012 e alle precisazioni contenute nei Piani nazionali anticorruzione 2015 e 2016). Diversamente il RPD può essere individuato in una professionalità interna all'ente o assolvere ai suoi compiti in base ad un contratto di servizi stipulato con persona fisica o giuridica esterna all'ente (art. 37 del Regolamento (UE) 2016/679). Fermo restando, quindi, che il RPCT è sempre un soggetto interno, qualora il RPD sia individuato anch'esso fra soggetti interni, l'Autorità ritiene che, per quanto possibile, tale figura non debba coincidere con il RPCT. Resta fermo che, per le questioni di carattere generale riguardanti la protezione dei dati personali, il RPD costituisce una figura di riferimento anche per il RPCT, anche se naturalmente non può sostituirsi ad esso nell'esercizio delle funzioni. Si consideri, ad esempio, il caso delle istanze di riesame di decisioni sull'accesso civico generalizzato che, per quanto possano riguardare profili attinenti alla protezione dei dati personali, sono decise dal RPCT con richiesta di parere al Garante per la protezione dei dati personali ai sensi dell'art. 5, co. 7, del d.lgs. 33/2013. In questi casi il RPCT ben si può avvalere, se ritenuto necessario, di un supporto del RDP nell'ambito di un rapporto di collaborazione tra le figure, ma limitatamente a profili di carattere generale, tenuto conto che proprio la legge attribuisce al RPCT il potere di richiedere un parere al Garante per la protezione dei dati personali. Ciò anche se il RPD sia stato eventualmente già consultato in prima istanza dall'ufficio che ha riscontrato l'accesso civico oggetto del riesame. Le considerazioni sopra espresse per le amministrazioni e gli enti valgono anche per i soggetti di cui all'art. 2-bis, co. 2, del d.lgs. 33/2013 tenuti a nominare il RPCT, qualora, ai sensi del Regolamento (UE) 2016/679, siano obbligati a designare anche il RPD.

Alla data di redazione del presente documento è stato preso in considerazione l'Organigramma di seguito riportato. Il documento di riferimento sarà in ogni caso l'Organigramma vigente.



§ 5. STRUTTURA DEL DOCUMENTO

Il presente documento è strutturato, come di seguito descritto, nella presente Parte Generale ed in una serie di allegati di Parte Speciale; queste ultime hanno ad oggetto, descrivono e disciplinano ambiti caratterizzati da maggiore dinamicità e che pertanto possono eventualmente essere soggette a e necessitare revisioni più frequenti.

A] Parte Generale, la quale integra:

(i) una disamina di carattere generale dei principi applicabili e della normativa di riferimento;

(ii) individua le procedure e le misure adottate e i principi giuridici, organizzativi e tecnici da rispettare affinché sia garantito il rispetto dei principi dettati dal Regolamento;

(iii) nonché le norme comportamentali a cui dovranno attenersi tutti gli incaricati del trattamento.

B] una serie di **allegati di Parte Speciale, ciascuno riferibile ai singoli uffici aziendali**:

Gli allegati contengono il **Registro delle attività di trattamento**, con puntuale individuazione dei seguenti elementi:

1. elenco dati, finalità, modalità di raccolta presso l'interessato e/o presso terzi, i termini ultimi di cancellazione,
2. le misure di sicurezza fisiche e logiche a tutela dei dati, adottate e/o da adottare,
3. i flussi interni e verso l'esterno dei dati, il titolare del trattamento, il responsabile del trattamento, l'eventuale responsabile esterno, i soggetti interessati e gli incaricati al trattamento. Con specifico riferimento ai flussi il dato è indicato primariamente nel registro dell'Ufficio che acquisisce in prima battuta il dato medesimo; ciò non fa venire meno l'obbligo in capo agli Uffici destinatari dei dati in virtù del Flusso cd. Interno, di trattare il dato conformemente alle procedure di riferimento.

Si precisa che le eventuali operazioni sui dati sono sostanzialmente di archiviazione ed estrapolazione: è del tutto assente qualsivoglia attività di profilazione.

Come noto il Registro dei Trattamenti sui dati personali è uno strumento indispensabile per gestire le informazioni in modo conforme al GDPR, ma anche per documentare e dimostrare tale conformità. L'istituzione del Registro delle attività serve a garantire il controllo della sicurezza sui dati personali; il diritto all'oblio, cioè il diritto ad ottenere la cancellazione dei propri dati personali quando non servono più alle finalità per cui erano stati forniti; la portabilità dei dati da un titolare ad un altro. Il registro quindi "*non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali*" (http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali). Per questo il Garante della Privacy ha invitato tutte le imprese ad istituire il registro, indipendentemente dalle loro dimensioni e/o dalla obbligatorietà in punto sua adozione. Il registro deve essere tenuto in forma scritta, anche in formato elettronico, e prevede i seguenti contenuti obbligatori (definiti nell'articolo 30 del GDPR):

- nome, cognome e contatti del Titolare del trattamento, del Responsabile del trattamento e del Responsabile della protezione dei dati (se nominati);
- finalità del trattamento dei dati ed operazioni sui dati;
- descrizione delle categorie di dati e delle categorie di interessati;
- descrizione dei flussi interni dei dati;

- descrizione delle categorie dei destinatari a cui saranno comunicati i dati personali (comprese imprese e sedi estere);
- indicazione dei trasferimenti di dati verso paesi esteri e organizzazioni internazionali, con identificazione dei destinatari;
- termini previsti per la cancellazione delle diverse categorie di dati;
- descrizione delle misure di sicurezza fisiche e logiche;
- previsione di procedure tecniche, organizzative e giuridiche per l'attuazione ed il rispetto delle disposizioni di cui al Regolamento.
  Al fine di una immediata comprensione del documento si evidenzia come tutti gli allegati abbiano struttura similare e contengano le medesime tabelle (a titolo esemplificativo tabella "*flusso esterno dati*"), anche laddove in concreto esse non risultino, ad oggi, applicabili -per assenza di flusso di dati- allo specifico ufficio preso in considerazione; in tal caso la tabella risulterà vuota, vale a dire priva di "*X*", che laddove presenti indicano, al contrario, il trattamento di quello specifico dato da parte dell'ufficio e/o il flusso dello stesso verso altri uffici. Si è infatti ritenuto che detta strutturazione permetta un più puntuale monitoraggio dello stato di conformità della Società alla normativa, avendo sempre presente gli obblighi a cui adempiere e la necessità di implementazione dei documenti in ipotesi di modifiche dell'assetto organizzativo e/o dei dati trattati.

Gli allegati dei singoli uffici individuano le seguenti figure:

Titolare del trattamento: Labcam, in persona del legale rappresentante *pro tempore*;

Responsabile del trattamento, in persona del titolare

Responsabile esterno del trattamento, laddove esistente

Interessati al trattamento: soggetti i cui dati sono oggetto di trattamento

Incaricati al trattamento: dipendenti o collaboratori della Società, adibiti ai singoli uffici, incaricati del trattamento dei dati

DPO: soggetto incaricato quale Responsabile Protezione Dati

C] Si precisa che sono state oggetto di rivisitazione le **informative** da fornire ai soggetti interessati. Ed infatti, oltre ad adeguare l'organizzazione aziendale, il nuovo regolamento GDPR richiede anche di aggiornare le informative sulla privacy. Gli utenti devono essere informati sull'utilizzo dei propri dati con un linguaggio chiaro e trasparente, facendo riferimento al "*GDPR General Data Protection Regulation- Regolamento UE 2016/679"*. L'informativa deve spiegare:

- in che modo e per quale scopo verranno trattati i propri dati personali;
- se il conferimento dei propri dati personali è obbligatorio o facoltativo;
- le conseguenze di un eventuale rifiuto a rendere disponibili i propri dati personali;
- a chi saranno comunicati o se saranno diffusi i propri dati personali;
- i diritti previsti dall'art. 7 del Codice;
- chi è il titolare e (se è stato designato) il responsabile del trattamento.

Per quanto sopra esposto i singoli allegati della documentazione in materia privacy comprendono, unitamente alla presente Parte Generale, il registro delle attività di trattamento e le procedure per l'adeguamento e l'osservanza del regolamento UE 2016/679 degli uffici.

D] I documenti sono stati adottati dal Direttore, al fine di una corretta e puntuale formalizzazione circa la loro adozione. Gli stessi sono sottoscritti per presa visione e al fine di garantire l'ottemperanza alle procedure riferibili ai singoli uffici dai dipendenti indicati quali incaricati del trattamento.

§ 6. PRINCIPI DA OSSERVARE NELLA RACCOLTA E NEL TRATTAMENTO DEI DATI

§ 6.1 RACCOLTA DATI E INFORMATIVA

I dati degli interessati raccolti dovranno essere trattati in modo lecito, corretto e trasparente.

A tal fine gli Incaricati del trattamento dovranno provvedere a predisporre un'adeguata informativa, da consegnare all'Interessato, redatta con un linguaggio semplice e chiaro, per iscritto o con mezzi elettronici, la quale dovrà riportare i seguenti elementi:

- l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

- i dati di contatto del responsabile della protezione dei dati, ove applicabile;

- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

- il diritto di proporre reclamo a un'autorità di controllo;

- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

- dovrà essere ben specificato quali autorizzazioni al trattamento dei dati sono obbligatorie per l'instaurazione ed esecuzione del rapporto di lavoro e quali invece sono facoltative e la durata dello stesso.

Gli Incaricati, data l'informativa, prima di procedere al trattamento dei dati, dovranno procedere a richiedere agli interessati il consenso al trattamento, provvedendo a richiedere specifiche autorizzazioni per ogni specifica attività di trattamento.

Il consenso non è dovuto qualora:

- i dati vengano trattati nell'esecuzione di un contratto o in fase pre-contrattuale;
- il trattamento venga fatto per dare esecuzione a un obbligo legale;
- i dati provengano da registri ed elenchi pubblici;
- i dati siano relativi allo svolgimento di attività economiche da parte dell'interessato.

La richiesta dei dati dovrà, inoltre, rispondere al **principio di minimizzazione**.

In base a tale principio si dovrà provvedere a raccogliere, per ciascun Interessato, i soli dati necessari per ogni specifica finalità di trattamento evitando di raccogliere dati sovrabbondanti.

Dovrà, inoltre, essere specificato nell'informativa, o con apposite policy aziendali, le modalità e finalità di raccolta e conservazione dei dati relativi all'uso della posta elettronica dei dipendenti.

I dati degli interessati dovranno essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.

A tal fine i Soggetti Incaricati dovranno limitare la richiesta dei dati agli interessati a quelli strettamente necessari per le finalità di cui al **Registro delle attività di trattamento**. Il Titolare del Trattamento, ed il Responsabile del Trattamento, se nominato, dovranno vigilare affinché il trattamento sia effettivamente effettuato solo per le finalità di cui al **Registro delle attività di trattamento**. Qualora sorgano esigenze di procedere al trattamento per diverse ed ulteriori finalità, tali finalità dovranno essere comunicate all'Interessato il quale, salvo i casi indicati di esonero dal consenso, dovrà esprimere uno specifico consenso per tale ulteriore trattamento. Tali ulteriori finalità dovranno essere specificate nell'informativa.

Nella fase di raccolta dei dati, soprattutto quelli sensibili, gli Incaricati del trattamento, nel caso di dubbio in merito alla necessità del trattamento di un determinato dato o della liceità dello stesso, dovranno coordinarsi con i consulenti esterni parte legale, medicina del lavoro, se applicabile, e Commercialista per ricevere istruzioni in merito al tipo e natura minima necessaria dei dati personali necessari per adempiere agli obblighi di legge.

I dati sensibili trattati in formato cartaceo dovranno essere archiviati in armadi muniti di chiave e non essere mai lasciati incustoditi. Di concerto con il consulente informatico dovranno essere adottate particolari misure di sicurezza a protezione dei dati sensibili trattati per mezzo di strumenti elettronici.

I dati raccolti dovranno essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («*esattezza*»).

A tal fine gli Incaricati del trattamento dovranno verificare l'esattezza dei dati forniti confrontandoli con quelli riportati nel documento di identità dell'Interessato.

All'Interessato dovrà essere comunicato un indirizzo e-mail specifico presso il quale comunicare eventuali variazioni o inesattezze dei propri dati personali.

In caso di richiesta di rettifica o di segnalazione di un errore di un dato personale giunta da un Interessato, l'Incaricato dovrà provvedere all'immediata modifica del dato presso il data-base ove il dato è presente, sia cartacea che informatica, tenendo nota, sia cartacea che informatica, dell'avvenuta modifica del dato e tenendo copia della e-mail ricevuta dall'interessato.

L'Incaricato dovrà, quindi, provvedere a comunicare la variazione del dato anche a tutti gli altri uffici ed ai soggetti terzi a cui il dato era stato precedentemente comunicato.

Le suddette operazioni dovranno essere eseguite al più presto e, comunque, non oltre 30 gg. dalla ricezione della richiesta da parte dell'Interessato.

Appena eseguite le operazioni di cui sopra l'Incaricato dovrà darne pronta comunicazione all'interessato riportando nel dettaglio la modifica eseguita e chiedendone ulteriore conferma.

Le procedure di cui sopra dovranno essere adottate anche qualora, in assenza di alcuna segnalazione, ci si rendesse conto che un dato, o le finalità per cui è stato raccolto, non è più necessario o conforme rispetto alle finalità per il quale viene trattato.

§ 6.2 Flussi dei Dati

§ 6.2.1 Flussi Interni

Anche all'interno della stessa organizzazione solo i soggetti incaricati del trattamento, e specificamente individuati, possono accedere e trattare i dati per le finalità per le quali sono stati raccolti.

Il flusso dei dati descritto nel **Registro delle attività di trattamento** deve essere l'unico ammesso. Ciò comporta che per ogni tipologia di dato possono avere accesso e trattarlo solo i soggetti incaricati indicati nel **Registro delle attività di trattamento**.

Devono essere adottate idonee misure sia fisiche che logiche affinché solo i soggetti incaricati come individuati nel **Registro delle attività di trattamento** possano avere accesso ai singoli dati in ragione del flusso dei dati descritto. In relazione ai dati in formato cartaceo solo i suddetti soggetti, quindi, potranno avere le chiavi dell'ufficio e degli armadi unitamente al responsabile del trattamento, se nominato, o del titolare del trattamento. In relazione ai dati in formato elettronico solo i suddetti soggetti potranno avere le credenziali di accesso ai dati informatici relativi ai dati per i quali sono incaricati al trattamento.

Nel caso in cui un diverso incaricato al trattamento, di un diverso ufficio non ricompreso nel flusso descritto nel **Registro delle attività di trattamento riferibile allo specifico Ufficio a cui si riferisce il registro**, avesse bisogno di uno dei dati tenuti in modalità cartacea o informatica, dovrà inviare e-mail motivata al DPO e all'organo Gestorio, il quale, se ritenuta fondata la richiesta, provvederà ad autorizzare, temporaneamente, e solo in ragione di specifici dati, il trattamento da parte del soggetto interno non ricompreso nel flusso dei dati descritto nel **Registro delle attività di trattamento**.

Le suddette misure andranno aggiornate ed adeguate in ragione delle innovazioni tecnologiche che interverranno ed in ragione di eventuali mutate esigenze di sicurezza conseguenti alla natura dei dati trattati ed alle attività di trattamento.

§ 6.2.2 Flussi verso l'Esterno

I dati dovranno essere comunicati al soggetto terzo solo per una o più delle finalità di cui al **Registro delle attività di trattamento** e, per le comunicazioni non dovute per adempiere ad obblighi di legge, solo previo consenso specifico rilasciato dall'interessato.

I dati trasmessi dovranno essere i minimi indispensabili per tali finalità.

Il soggetto a cui verranno comunicati i dati dovrà dare idonee garanzie al fine di rispettare i principi contenuti nel Regolamento in merito al trattamento dei dati, al rispetto dei diritti dell'interessato e nell'adozione delle misure di sicurezza a tutela dei dati.

Il flusso dei dati esterno descritto nel **Registro delle attività di trattamento** deve essere l'unico ammesso per tipologia di dato e per finalità.

Nei rapporti contrattuali con i terzi ai quali verranno comunicati i dati dovranno essere ineriti specifici obblighi da parte del terzo affinché questo, nel trattamento dei dati comunicati, si impegni a rispettare i principi contenuti nel

Regolamento in merito al trattamento dei dati, al rispetto dei diritti dell'interessato, ivi inclusa la portabilità dei dati, e nell'adozione delle misure di sicurezza a tutela dei dati.

Lo stesso contratto dovrà contenere, altresì, l'impegno del terzo a sottoporsi ad audit organizzati dal titolare del trattamento per verificare il rispetto dei suddetti principi e misure di sicurezza, prevedendo la risoluzione contrattuale nel caso di loro violazione.

Per ciascun soggetto terzo come sopra identificato sarà necessario, inoltre, tracciare tutte le operazioni di sub-trattamento, ovvero richiedere a ciascun terzo per iscritto, ottenendone risposta scritta, a quali soggetti a sua volta comunica i dati ad esso trasferiti dalla società e provvedere, quindi, ad inserire tali informazioni nel presente documento aggiornandole periodicamente.

§ 6.2.2.1 FLUSSI VERSO L'ESTERNO: TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI SITI AL DI FUORI DELLO SPAZIO EUROPEO

In seguito all'analisi svolta al momento della redazione ed approvazione del presente Modello è emerso che, allo stato, la Società non trasferisce dati verso paesi terzi al di fuori dei paesi UE (tutt'al più riceve informative da soggetti residenti in detti stati).

Il Titolare del trattamento e il Responsabile del trattamento ed il Responsabile per la Protezione dei Dati, se nominati, provvederanno ad una verifica costante dei flussi informativi verso soggetti terzi per verificare se si verificano altri trasferimenti verso paesi terzi, con particolare attenzione ai dati tenuti in servizi di cloud gestiti da terzi o comunque da provider con server siti in paesi terzi extra UE.

Provvedendo al trasferimento di dati verso paesi terzi dovranno essere adottate le seguenti misure

- assicurarsi che il paese terzo in questione garantisca i medesimi livelli di tutela garantiti dall'Unione Europea in seguito ad una dichiarazione di adeguatezza in tal senso emanata dall'Unione;
- Il soggetto terzo, a prescindere dai livelli di tutela garantiti dal paese ove è sito, fornisca garanzie adeguate. Nel caso di trasferimento dati verso soggetti residenti in USA, assicurarsi che l'azienda in questione abbia aderito al Privacy Shield (IP/16/216);
- Prevedere adeguate forme di tutela contrattuali con il soggetto sito in un paese terzo;

Se presenti le suddette garanzie, la relativa documentazione delle stesse dovrà essere allegata al presente Modello.

In mancanza della suddetta dichiarazione di adeguatezza, o di verifica delle suddette garanzie, i dati potranno essere comunque trasmessi verso un paese terzo extra UE qualora:

- l'Interessato abbia espressamente acconsentito al trasferimento dopo essere stato adeguatamente avvertito dei rischi derivanti dalla mancata verifica di adeguatezza o della insussistenza delle suddette garanzie;
- il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato ed il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;
- il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica e giuridica a favore dell'interessato;
- il trasferimento sia necessario per importanti motivi di interesse pubblico;

- il trasferimento sia necessario per accertare, esercitare, o difendere un diritto in sede giudiziaria;
- il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'Interessato si trovi nell'impossibilità fisica o giuridica di prestate il proprio consenso;
- il trasferimento sia effettuato partendo da un registro pubblico consultabile dal pubblico o da chi dimostra di avere un legittimo interesse.

Nel caso in cui non ricorra nessuno dei suddetti presupposti il trasferimento verso un paese terzo extra UE potrà avvenire solo se:

- non è ripetitivo;
- riguarda un numero limitato di interessati;
- è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato;
- qualora il titolare e del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali;
- il titolare del trattamento informa del trasferimento il Garante privacy.

In ogni caso, qualora vengano trasferiti dati in paesi terzi extra UE, il Titolare dovrà riportare nel presente modello (allegato REGISTRO DELI TRATTAMENTI) quali tipi di dati riferiti a quali categorie di interessati vengono trasferiti ed identificare i soggetti ai quali vengono trasferiti.

§ 7. MISURE DI SICUREZZA A TUTELA DEI DATI

Gli Uffici adottano le **misure di sicurezza** riportate nel **Registro delle attività di trattamento** a ciascun ufficio riferibile.

Si evidenzia come le attività vengano svolte, per il tramite dei dipendenti, presso le seguenti sedi:

- **ALBENGA** Regione Rollo, 98 - CAP 17031 Albenga (SV)
- **PIACENZA** – (limitatamente per la seguente attività) Sportello ricezione campioni Labcam **presso Aeiforia** Loc. Faggiola 12-16 I-29027 Gariga di Podenzano (PC)
- **CAGLIARI** via Polvani 2- 09067 zona industriale Elmas

Con riferimento alle misure di sicurezza "fisica" (ingresso presidiato, servizio di vigilanza, videosorveglianza ingresso principale immobile, sistema antincendio, sistema d'allarme, armadi muniti di chiavi, porta uffici munita di chiave, porta CED munita di chiave) nel Registro dei Trattamenti viene dato atto delle differenti misure presenti presso le singole unità.

Del pari sono oggetto di analisi le misure di sicurezza logiche (Anti virus PC, Anti Virus server, Firewall Server, Back-up automatici, Profili di autenticazione per aree, Disaster recovery, Server Ridondanti, Pseudonimizzazione dei dati, Sistema di alert e monitoraggio violazioni).

Il Titolare del trattamento, ed il Responsabile del trattamento, se nominato, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

§ 8. IL RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI

L'art.37 del Regolamento, rubricato "*Designazione del responsabile della protezione dei dati*" (il quale individua le ipotesi in cui ricorre l'obbligo di nomina di un Responsabile per la Protezione dei Dati (RPD)) recita:

«*1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:*

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.

3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.

5. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo».

La Società rientra –cautelativamente e trattandosi di soggetto in controllo di Camera di Commercio- nei casi previsti dall'art. 37, par. 1, lett. a) del Regolamento (UE) 2016/679. La Società ha quindi provveduto alla nomina del RPD / DPO. Si ricorda che solo in ipotesi la scelta del RPD ricada su una professionalità interna all'ente, occorra formalizzare un apposito atto di designazione a "*Responsabile per la protezione dei dati*". Laddove, invece, si ricorra a soggetto esterno all'ente legato alla Società da un rapporto di consulenza –come nel caso di specie- la designazione costituirà parte integrante dell'apposito contratto di servizi redatto in base a quanto previsto dall'art. 37 del RGPD.

Il Titolare del trattamento o il Responsabile provvederanno a rendere noto in modo idoneo agli Interessati, a tutti i dipendenti ed al Garante Privacy, i dati di contatto dell'eventuale RPD.

A RPD dovranno essere concessi adeguati mezzi finanziari e strumenti per adempiere adeguatamene alla sua funzione e dovrà essere coinvolto nelle decisioni aziendali che possano influire sui dati personali ed in particolare:

- dovrà essere convocato ogni qualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati, richiedendo allo stesso un parere in merito;
- dare sempre la dovuta considerazioni ai suoi pareri;
- procedere ad una tempestiva consultazione nel caso di violazione dei dati.

L'indipendenza del RPD e l'assenza di situazioni di conflitto risulta garantita dal ricorso a professionalità esterna e non è risultato necessario adottare le specifiche misure previste in ipotesi di nomina di soggetto legato alla Azienda da rapporto di dipendenza (gestione rapporti con superiori gerarchici, rimozione del RPD etc.).

§ 9. VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Al momento della redazione ed approvazione del presente modello Labcam non rientra tra i soggetti obbligati.

Il titolare del trattamento ed il Responsabile del trattamento ed il Responsabile per la Protezione dei dati personali provvederanno a monitorare periodicamente la tipologia dei dati trattati e le modalità di trattamento al fine di verificare se la Società rientra nel suddetto obbligo. Ovvero se ricorrono i seguenti presupposti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 Regolamento, o di dati relativi a condanne penali e a reati di cui all'articolo 10 Regolamento;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il titolare del trattamento ed il Responsabile del trattamento ed il Responsabile per la Protezione dei dati personali, se nominati provvederanno a verificare periodicamente se l'autorità di controllo provvederà ad aggiornare e rende pubblico il suddetto elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati.

Nel caso in cui ricorrano i suddetti presupposti il Titolare adotta le seguenti misure.

Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati;

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Nel valutare l'impatto del trattamento effettuato dal Titolare o dal responsabile, dovranno tenere in debito conto il rispetto dei codici di condotta approvati di cui all'articolo 40 Regolamento, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

Se del caso, il titolare del trattamento raccoglierà le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

Qualora la suddetta valutazione d'impatto indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio, il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo.

L'autorità di Controllo, se ritiene che il trattamento violi il Regolamento e ritenga che il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, fornirà, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento. Tale periodo potrà essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informerà il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

Al momento di consultare l'autorità di controllo il titolare del trattamento dovrà comunicare a questa:

a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;

b) le finalità e i mezzi del trattamento previsto;

c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;

d) ove applicabile, i dati di contatto del titolare della protezione dei dati;

e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35 Regolamento;

f) ogni altra informazione richiesta dall'autorità di controllo.

§ 10. I DIRITTI IN CAPO ALL'INTERESSATO

§ 10.1 RICHIESTA DI ACCESSO AI DATI

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 Regolamento, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 Regolamento relative al trasferimento.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento.

In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia dei dati personali oggetto di trattamento non deve ledere i diritti e le libertà altrui.

Ricevuta una richiesta di accesso ai dati personali proveniente da un Interessato, l'Incaricato, previo accertamento che la richiesta provenga dall'effettivo interessato, provvederà ad avvertire, senza indugio, il Titolare ed il Responsabile del trattamento, se nominato, e provvedere, quindi, a fornire all'Interessato le informazioni richieste per iscritto nel formato più idoneo ed accessibile.

§ 10.2 Richiesta di Cancellazione dei Dati

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento;

c) l'interessato si oppone al trattamento;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione;

Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1 Regolamento, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

Per essere conformi ai suddetti principio si adottano le seguenti misure: una volta decorsi i termini di trattamento relativi a ciascun dato riportati nel Registro delle attività di trattamento si dovrà procedere alla cancellazione di tali dati sia in formato cartaceo che digitale. Qualora ci sia il rischio che la cancellazione possa comportare una violazione di legge o pregiudicare i diritti della società, dell'Interessato o di terzi, il Responsabile del trattamento interroga sul punto l'RPD, se nominato, o in mancanza, il consulente esterno.

Il Titolare del trattamento, di concerto con il Responsabile del trattamento, se nominato, coadiuvati dal RPD, se nominato, provvederanno ad individuare le categorie di dati che andranno cancellati o resi anonimi ricorrendone i suddetti presupposti, e le migliori procedure perché tale misura sia attuata.

Inoltre qualora giunga una richiesta di cancellazione o di opposizione al trattamento da parte di un interessato al trattamento l'incaricato dovrà subito darne informazione al Responsabile del Trattamento.

Questi provvederà, senza indugio, a valutare, anche tramite consulenti esterni, la sussistenza del diritto alla cancellazione e che tale cancellazione non comporti violazioni di legge, e non pregiudichi i diritti dell'Interessato o di terzi e, in caso affermativo, a provvedervi nei tempi più brevi individuando le modalità più idonee.

§ 10.3 LIMITAZIONE DEL TRATTAMENTO DEI DATI

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 Regolamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento è limitato a norma dell'art.21 paragrafo 1 Regolamento, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

L'interessato che ha ottenuto la limitazione del trattamento a norma dell'art.21 paragrafo 1 Regolamento è informato dal titolare del trattamento prima che detta limitazione sia revocata.

Per essere conformi al summenzionato principio, qualora giunga una richiesta di limitazione del trattamento da parte di un interessato al trattamento, l'incaricato dovrà subito darne informazione al Responsabile del Trattamento, se nominato o, in mancanza, al Titolare del trattamento.

Questi provvederà, senza indugio, a valutare, anche tramite consulenti esterni, la sussistenza del diritto alla limitazione del trattamento e, in caso affermativo, a provvedervi nei tempi più brevi e secondo le modalità più idonee.

§ 10.4 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 forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a) Regolamento, o dell'articolo 9, paragrafo 2, lettera a) Regolamento, o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b) Regolamento;

b) 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.

Il suddetto diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

L'esercizio del suddetto diritto non deve ledere i diritti e le libertà altrui.

Per essere conformi al summenzionato principio, qualora giunga una richiesta di portabilità dei dati da parte di un interessato al trattamento, l'incaricato dovrà subito darne informazione al Responsabile del Trattamento, se nominato, o, in mancanza, al titolare del trattamento.

Questi provvederà, senza indugio, a valutare, anche tramite consulenti esterni, la sussistenza del diritto alla portabilità dei dati e che tale richiesta di portabilità non leda i diritti e le libertà altrui e, in caso di accertata sussistenza del diritto, e che il suo esercizi non pregiudichi i diritti di terzi, a provvedervi nei tempi più brevi e secondo le modalità più idonee.

§ 10.5 Opposizione al Trattamento

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) Regolamento, compresa la profilazione sulla base di tali disposizioni.

Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di 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 al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

Il diritto di cui all'art.21 paragrafi 1 e 2 Regolamento è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1 Regolamento, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Per essere conformi al summenzionato principio qualora giunga una richiesta di opposizione al trattamento da parte di un interessato al trattamento, l'Incaricato dovrà subito darne informazione al Responsabile del Trattamento, se nominato o, in mancanza, la titolare del trattamento.

Questi provvederà, senza indugio, a valutare, anche tramite consulenti esterni, la sussistenza del diritto all'opposizione al trattamento e che tale richiesta di opposizione non sia in contrasto con la necessità di trattare il dato per eseguire un compito di interesse pubblico e, in caso di accertata sussistenza del diritto e che il suo esercizi non pregiudichi l'interesse pubblico, a provvedervi nei tempi più brevi e secondo le modalità più idonee.

§ 11. Notifica di una Violazione dei Dati Personali all'Autorità di Controllo

Per violazione si intende una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica o la divulgazione non autorizzata, o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Per essere conformi al summenzionato principio è necessario adottare un sistema di monitoraggio dei dati che registri eventuali violazioni o tentativi di violazioni esterne ai sistemi informatici con un sistema di *allert* che comunichi la violazione, o il tentativo di violazione, al Responsabile del Trattamento e/o, se nominato, al RPD. Egualmente il sistema di monitoraggio registro ed *allert* dovrà monitorare, registrare ed avvertire i suddetti soggetti qualora vi sia una violazione interna rappresentata da operazioni anomale sui dati attuate dagli incaricati del trattamento.

Ferme restando le suddette misure qualora un qualsiasi dipendente si accorga, o sia a conoscenza di una violazione, sia interna che esterna, dei dati personali trattati dal Titolare, se non ne è già informato, dovrà subito darne informazione al Responsabile del Trattamento e/o, se nominato, al RPD.

In caso di violazione dei dati personali, il Responsabile del Trattamento notifica la violazione all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dai motivi del ritardo.

La notifica dovrà riportare nel dettaglio tutta la situazione, nonché i dati dei titolari e dei responsabili del trattamento, le probabili conseguenze della violazione stessa e quali misure sono state o si intende adottare per farvi fronte.

§ 12. Comunicazione di una Violazione dei Dati Personali all'Interessato

I presupposti sono rappresentati da una violazione di sicurezza che comporta accidentalmente o in modo illecito, la distruzione, la perdita, la modifica o la divulgazione non autorizzata, o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Per essere conformi al summenzionato principio è necessario adottare un sistema di monitoraggio dei dati che registri eventuali violazioni o tentativi di violazioni esterne ai sistemi informatici con un sistema di *allert* che comunichi la violazione, o il tentativo di violazione, al Responsabile del Trattamento e/o, se nominato, al RPD. Egualmente il sistema di monitoraggio registro ed *allert* dovrà monitorare, registrare ed avvertire i suddetti soggetti qualora vi sia una violazione interna rappresentata da operazioni anomale sui dati attuate dagli incaricati del trattamento.

Ferme restando le suddette misure qualora un qualsiasi dipendente si accorga, o sia a conoscenza di una violazione, sia interna che esterna, dei dati personali trattati dal Titolare, se non ne è già informato, dovrà subito darne informazione al Responsabile del Trattamento e/o, se nominato, al RPD.

Nei casi in cui la violazione dei dati personali può comportare un rischio elevato per i diritti e le libertà delle persone fisiche, il Responsabile del Trattamento, dovrà darne comunicazione all'interessato senza ingiustificato ritardo, con un linguaggio semplice e comprensibile.

La comunicazione deve contenere:

a) il nome ed i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
b) descrivere le probabili conseguenze della violazione dei dati personali;
c) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La suddetta comunicazione non sarà necessaria qualora il titolare del trattamento abbia messo in atto misure tecnico-organizzative adeguate di protezione (es. la cifratura), se ha adottato misure che hanno scongiurato il rischio per gli interessati ovvero quando la comunicazione richiederebbe sforzi sproporzionati. In tale ultimo caso è sufficiente comunicare pubblicamente la notizia, in modo tale che gli interessati ne vengano a conoscenza ugualmente.

Per limitare il rischio applicare il principio di minimizzazione dei dati in fase di raccolta e fare una valutazione del rischio. Per mezzo di tale valutazione bisognerà valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e della evoluzione delle fonti di rischio specie informatiche (ramsoware, virus, trojan); occorre valutare anche il rischio per i cittadini ed utenti e verificare se è elevato (es. quando si tratti di frode, furto di identità, danno all'immagine, dati giudiziari o sanitari).

§ 13. Informativa – Formazione e Procedure Operative

Il presente modello organizzativo (ed i suoi allegati) dovrà essere portato a conoscenza, ed attuato, da tutto il personale ed i collaboratori della società.

Il presente modello organizzativo, comprensivo degli allegati, dovrà essere aggiornato costantemente in ragione di qualunque modifica avvenga rispetto alla situazione tecnica, organizzativa e procedurale ivi decritta, o in seguito a mutamenti normativi o regolamentari in tema di dati personali, sia a livello nazionale che comunitario, nonché in ragione di qualunque modifica avvenga relativamente alla tipologia dei dati trattati ed alle attività o modalità di trattamento dai dati.

Nell'ottica di diffondere le conoscenze relative alla materia e di fornire adeguate istruzioni a tutto il personale sono realizzati, su proposta del DPO, progetti formativi specifici:

- per i dipendenti e i collaboratori in relazione al ruolo di "incaricati del trattamento";
- per le figure che ricoprono incarichi di responsabilità.

I dipendenti e collaboratori di Labcam potranno inoltre fare riferimento direttamente al RPD per la proposta di quesiti, la richiesta di approfondimenti e la tutela dei propri dati personali.

Specifiche attività di formazione/informazione saranno programmate al momento dell'assunzione di nuove risorse, nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento di dati personali.

La redazione e diffusione di disposizioni scritte ("*Procedure Operative*") che specificano e/o descrivono le modalità di esecuzione di un'attività e le regole di comportamento cui attenersi nello svolgimento dei compiti assegnati rappresentano un importante strumento per l'applicazione dei principi e delle disposizioni normative: le stesse dovranno essere scrupolosamente rispettate da parte dei destinatari del presente Modello.

§ 14. APPENDICE – DEFINIZIONI

Ai fini del Regolamento s'intende per:

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

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

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

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

5) «*pseudonimizzazione*»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali

informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

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

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

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

9) «*destinatario*»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati 4.5.2016 L 119/33 Gazzetta ufficiale dell'Unione europea IT membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

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

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

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

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

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

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

16) «*stabilimento principale*»: a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento

nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

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

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

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

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

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

22) «*autorità di controllo interessata*»: un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;

23) «*trattamento transfrontaliero*»: a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «*obiezione pertinente e motivata*»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «*servizio della società dell'informazione*»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (1);

26) «*organizzazione internazionale*»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Titolare del trattamento: Labcam Srl

- Responsabile del trattamento: il Titolare

Interessati al trattamento:

- Dipendenti;
- Collaboratori;

Incaricati al trattamento sig.ri:

- come individuati nelle Parti Speciali

Responsabile esterno del trattamento:

- come individuati nelle Parti Speciali

ALLEGATI

- REGISTRO DEL TRATTAMENTO RELATIVO ALLE SINGOLE AREE ED UFFICI
- PROCEDURA DI GESTIONE DEI DATA BREACH E REGISTRO DELLE VIOLAZIONI - DATA BREACH
- TAVOLA DI RAFFRONTO INFORMATIVE EX ART. 13 TU PRIVACY - EX ARTT. 13 E 14 GDPR
- ELENCO SOGGETTI INCARICATI
- ELENCO RESPONSABILI ESTERNI DEL TRATTAMENTO