Coopservice soc.coop. p.a con sede legale in via Rochdale 5 Reggio Emila RE, P.IVA 00310180351, in recepimento della normativa in tema di trattamento dei dati personali (UE GDPR 679/16, D.lgs.196/03 modificato dal D.Lgs. 101/18) aderisce al seguente modello di compliance:

A. Rappresentanza e contatti di Coopservice in ambito di trattamento dei dati personali

Coopservice Soc. Coop. P. A., considerata sia nella sua veste di Titolare del trattamento sia in quella di Responsabile per trattamenti eseguiti per conto di terzi Titolari:

- è rappresentata da Direttore Generale e procuratore speciale *pro-tempore* Michele Magagna,
- è contattabile all'indirizzo mail servizio.privacy@pec.coopservice.it , con sede legale in via Rochdale 5;
- Il Data Protection Officer è contattabile all'indirizzo mail dpo@coopservice.it.
- Le funzioni ITS (IT Security management) e ITO (IT Organization) sono contattabili tramite la funzione privacy alla casella mail ufficio.privacy@coopservice.it ovvero rivolgendosi al Data Protection Officer all'indirizzo mail: dpo@coopservice.it

Il Modello Organizzativo Privacy di Coopservice ha individuato la figura del Delegato ex art. 29 GDPR e art.2 quaterdecies Codice Privacy testo vigente, nella figura del proprio Direttore Operations, con facoltà di sub delega ai Direttori delle specifiche linee di servizio. La Funzione Privacy è integrata come unità specializzata all'interno dei Servizi Legali.

B. Recepimento del GDPR (UE GDPR 2016/679)

Coopservice Soc. Coop. P.A ha adottato un piano di recepimento del Regolamento Europeo, volto all'attuazione dei seguenti obiettivi primari:

- Registro dei trattamenti
- Analisi dei rischi & Data Protection Impact Assessment
- Misure di sicurezza IT & Rilevamento e Prevenzione incidenti di sicurezza
- Procedure per la notifica degli incidenti all'Autorità di Controllo ed agli interessati
- Revisione contratti di fornitura ex art. 28 GDPR
- attribuzione ruoli privacy interni (designati e autorizzati) ex art. 29 GDPR
- formazione di referenti privacy e degli autorizzati al trattamento ex art. 29 GDPR (aula o FAD)
- individuazione e designazione del Data Protection Officer (DPO) o Responsabile della protezione dei dati (RPD)
- definizione di un Modello di Privacy Governance, con individuazione, oltre al DPO, di figure delegate ex art. 29 GDPR, della Funzione Privacy, costituzione di un Gruppo di Lavoro Privacy (coordinato dalla Funzione Privacy e composto dai rappresentanti delle funzioni aziendali coinvolte nei processi a cui è connesso un trattamento di dati personali, quali Risorse Umane, Ufficio Clienti, Ufficio Fornitori, Ufficio Tecnico e Progettazione, Ufficio Gare, IT Security, Tecnologie Sicurezza e settore Security Solution).

C. Trattamenti di dati personali nella titolarità della committenza

Per i trattamenti di dati personali svolti per conto del Committente, Coopservice è qualificabile come responsabile del trattamento. I suoi compiti e le sue responsabilità in termini di conformità al GDPR, in quanto strettamente legati al diretto adempimento delle obbligazioni assunte e nei limiti anche tecnologici delle stesse, saranno oggetto apposito accordo ai sensi e nelle forme dell'art. 28 GDPR. Nella sua posizione di responsabile, Coopservice:

1. individuerà al proprio interno una o più funzioni che assicureranno, dal punto di vista organizzativo ed operativo, gli adempimenti previsti o concordati, relativamente ai trattamenti connessi ai servizi erogati;
2. individuerà gli autorizzati del trattamento, provvedendo – attraverso le competenti funzioni aziendali - alla loro formazione, in particolare a fronte di trattamenti considerati particolarmente rischiosi per i diritti degli interessati ed in caso di innovazione tecnologica, alla verifica della rispondenza delle operazioni di trattamento alle finalità stabilite dal Titolare terzo;
3. coinvolgerà nel trattamento fornitori di cui abbia verificato la affidabilità, nel caso in cui intendesse avvalersi di soggetti esterni quali sub-responsabili, informandone il Titolare e ottenendone la preventiva autorizzazione;
4. procederà con cadenza almeno annuale all'aggiornamento della lista degli incaricati ed alla verifica delle autorizzazioni allo specifico ambito di trattamento considerato;
5. individuerà ed adotterà le misure di sicurezza adeguate per proteggere i trattamenti cartacei o elettronici nella titolarità di terzi, eventualmente eseguiti con strumenti ed apparati nel proprio dominio e/o oggetto di fornitura, oltre alle procedure per la verifica ed il mantenimento delle misure adottate;
6. adotterà procedure per la segnalazione tempestiva di eventuali violazioni di sicurezza (data breach);
7. fornirà al Titolare tutte le informazioni a propria disposizione, tenuto conto del trattamento ed in ragione del proprio grado di coinvolgimento nella sua esecuzione, assistendolo nello svolgimento della valutazione d'impatto, ove questi vi debba procedere ai sensi dell'art. 35 GDPR.

D. Privacy by design dei servizi erogati

Per i trattamenti di dati personali nella titolarità di terzi (svolti quale responsabile ex art. 4 punto 8 GDPR), Coopservice adotta procedure e strumenti tecnici ed organizzativi funzionali ad incorporare gli aspetti di protezione e sicurezza dei dati personali nel ciclo dei servizi (**privacy by design / by default**), con particolare attenzione agli aspetti relativi alle seguenti disposizioni del GDPR:

- art. 28 comma 1, 2 e 4 (individuazione e accordo con il sub-responsabile, in caso di subappalto o subaffidamento, ricorso a fornitori critici),
- art. 29 (autorizzazione operatori che trattano dati personali, formazione e istruzioni),
- art.32 (analisi dei rischi secondo metodo oggettivo e best pratices di settore, per trattamenti effettuati con strumenti, mezzi o materiali, organizzazione proprie, individuazione e attuazione delle misure a contrasto dei suddetti rischi, monitoraggio e miglioramento delle misure adottate).
- art.33 comma 2 (segnalazione al titolare di eventuali violazioni di sicurezza subite, in relazione ai trattamenti affidati).

E. Integrazione degli aspetti di privacy compliance nel sistema di gestione integrato QASRS

Gli aspetti di compliance alla vigente normativa a tutela dei dati personali sono stati integrati nel sistema di gestione per la Qualità, l'Ambiente, la Salute e la Sicurezza sul Lavoro e la Responsabilità Sociale (certificato a fronte delle norme UNI EN ISO 9001:2015, UNI EN ISO 14001:2015; UNI ISO 45001:2018; SA 8000:2014; per le attività di sicurezza e vigilanza privata: UNI 10891:2000; UNI 50518:2014; UNI EN 16082:2011; per la prevenzione della corruzione ISO 37001) , in particolare all'interno delle seguenti procedure:

- P03 - Erogazione del servizio: procedure, istruzioni e metodiche per il trattamento di dati personali negli uffici e nei cantieri di erogazione del servizio;
- P04 - Approvvigionamenti e P04.1 Subappalti: procedure per la compliance dei profili inerenti il trattamento di dati personali nella trattati da terzi per conto di Coopservice nelle forniture di servizi e consulenze, tecnologie e strumenti;
- P05 - Gestione delle Risorse Umane: procedure, istruzioni e metodiche per la gestione degli autorizzati del trattamento ex art. 29 GDPR.
- P08 - Gestione della documentazione: responsabilità per la gestione della documentazione a tutela dei dati personali.
- P09 - Gestione delle non conformità per la gestione di segnalazioni interne o esterne di anomalie sulla tutela dei dati personali
- P11 - Gestione delle verifiche ispettive interne, per il sistema di verifica degli adempimenti e delle procedure interne
- P15 - Gestone delle prescrizioni legali per intercettare e recepire le modifiche normative

Gli aspetti sono verificati nel corso degli audit interni di sistema e sono oggetto di specifiche verifiche e implementazioni da parte di professionisti esterni certificati. I risultati dei controlli sono comunicati alle funzioni privacy interne ed esterne (Funzione Privacy, Gruppo di Lavoro Privacy, DPO, Delegati, Direzione Generale), che procedono al riesame intraprendendo le eventuali azioni correttive.

F. Monitoraggio dei trattamenti di dati personali e valutazione di impatto

In ossequio alle sopra citate procedure, l'implementazione di servizi, l'acquisto di beni, lo sviluppo di soluzioni tecnologiche sono oggetto di valutazione in ordine allo specifico trattamento ad esse correlato, sia sotto il profilo del compliance ai principi fondamentali del Regolamento Europeo (capo II GDPR art.5 e ss.) sia sotto il profilo del probabile rischio per i diritti e le libertà degli interessati. Laddove questo rischio si presenta elevato, si procede a valutazione d'impatto ai sensi dell'art.35 GDPR (metodologa preferenziale CNIL). I trattamenti soggetti a DPIA sono periodicamente oggetto di riesame. In caso di nuovi trattamenti o di variazioni in quelli esistenti, si procede ad aggiornare il Registro ex art. 30 comma 1 e 2 GDPR e le informative ex art.13 GDPR e 14 GDPR correlate.

G. Misure di Sicurezza

Nell'esecuzione dei trattamenti in proprio o connessi a servizi oggetto di contratto, secondo la correlazione processi / servizi / trattamenti attuata nel proprio Privacy Business Model, Coopservice attua misure organizzative e tecniche adeguate (art. 32 GDPR) a garantire la sicurezza, la disponibilità e l'integrità delle informazioni, nonché le libertà ed i diritti degli interessati, a tal fine procedendo periodicamente ad una analisi dei rischi (art. 32 comma 2 GDPR) basata su metodi e procedure oggettive o standardizzate (ad oggi viene adottato un metodo basato su *guidelines* ENISA).

H. Organizzazione del personale e autorizzazioni al trattamento:

Il personale che tratta dati personali è autorizzato da Coopservice SCPA ai sensi dell'art.29 GDPR. Il personale tecnico (sistemi informativi Coopservice) è individuato quale amministratore di sistema. Il personale - anche non autorizzato - è vincolato formalmente con impegni di riservatezza e riceve istruzioni comportamentali specifiche, atte a tutelare qualsiasi informazione e notizia di qualsiasi tipologia, a chiunque riferita, indipendentemente dalle modalità e dalle circostanze in cui dette informazioni sono apprese, con particolare riferimento a informazioni, confidenze e notizie coperte dal segreto aziendale di Coopservice, del Committente o di terzi oppure aventi natura riservata ex lege o di fatto.

Le procedure per la gestione degli autorizzati sono integrate nel sistema QASRS adottato da Coopservice (in particolare P05 "Gestione delle risorse umane") e relative metodiche e istruzioni operative. La correlazione tra le categorie dei dati e quelle dei soggetti autorizzati a trattarli è definita in una Matrice degli Incaricati al Trattamento (MIT), periodicamente aggiornata.

Nelle lettere di autorizzazione al trattamento (distribuite al personale al momento dell'assunzione ed aggiornate secondo evoluzione normativa o esigenze legate a specifici trattamenti successivamente autorizzati) sono state inserite istruzioni e indicazioni sui comportamenti da seguire sia per il corretto trattamento dei dati, sia per l'utilizzo degli strumenti in dotazione. L'utilizzo del sistema informatico Coopservice da parte degli utenti è inoltre regolamentato dal Disciplinare Informatico Aziendale (DIA) periodicamente aggiornato, a disposizione di tutti gli utenti.

I. Formazione

Gli Autorizzati ricevono una formazione sul trattamento di dati personali in modalità FAD. Laddove necessario o in caso di approfondimenti, sono organizzate sessioni in aula o viene fornito supporto formativo documentale ad hoc. Gli amministratori di sistema sono formati con sessioni in aula. Per il personale autorizzato di staff e il personale tecnico, oltre ai moduli precedenti, sono pubblicati in modalità FAD moduli specifici per le aree tematiche di rispettivo interesse.

J. Impegno di riservatezza

Tutto il personale (anche non autorizzato al trattamento ex art. 29 GDPR) è vincolato alla riservatezza e riceve istruzioni comportamentali specifiche, atte a tutelare non solo i dati personali come definiti dalla normativa europea o nazionale ma qualsiasi informazione e notizia non trattata da Coopservice ai sensi dell'art. 28 GDPR, con particolare riferimento a informazioni, confidenze e notizie:

- coperte dal segreto aziendale di Coopservice, del Committente o di terzi (per es. procedure e metodiche di produzione, principi di funzionamento di mezzi e macchinari, progetti, prototipi in fase di collaudo o di sperimentazione, ecc…);
- aventi natura riservata ex lege o di fatto (per es. notizie e fatti relativi a trattative contrattuali, situazioni finanziarie ed economiche, piani e strategie di impresa, indiscrezioni su indagini, controversie o procedimenti, codici di accesso ad aree riservate, ecc….)

K. Diritti degli interessati e contatti del DPO

Come indicato nelle informative ex art.13 GDPR e 14 GDPR, per agevolare la pronta presa in carico delle richieste degli interessati e l'esercizio dei loro diritti (artt.15 ess. GDPR) viene istituito come punto di contatto la Funzione Privacy / referente del DPO (ufficio.privacy@coopservice.it oppure dpo@coopservice.it). È altresì possibile contattare il DPO o inviare una segnalazione nell'apposita sezione contatti del sito WEB aziendale (https://www.coopservice.it/invia-segnalazione-dpo).

L. Data Breach

Coopservice adotta uno specifico protocollo per definire ed attuare i criteri ed i processi per il rilevamento, l'individuazione e la gestione di una violazione di sicurezza delle informazioni che rientra nella definizione di Data Breach ai sensi dell'articolo 4 punto 12 del GPDR.

Il suddetto protocollo si applica a:

- tutti i contesti societari (Sede, Filiali, Cantieri e Postazioni presso il cliente);
- tutte le attività e i processi che comportano un trattamento di dati personali eseguito da Coopservice come Titolare del trattamento o come Responsabile di trattamenti eseguiti per conto di terzi Titolari (clienti, partner o fornitori);
- tutti i soggetti, sia interni che esterni alla Società indipendentemente dal ruolo, dalle mansioni ricoperte e dalle responsabilità affidate.

La gestione di un evento può essere suddivisa nelle seguenti fasi:

I. Rilevamento, analisi e classificazione:
   1. Rilevazione e segnalazione mediante canali pre-configurati e key people;
   2. Analisi e classificazione dell'incidente secondo livelli crescenti: (I) falso positivo, (II) tentativo di violazione, (III) incidente di sicurezza, (IV) violazione di dati personali;

II. Identificazione del data breach
   3. Stato di allerta. Accertamento del data breach
   4. Attivazione del Breach Response Team;
   5. Analisi tecnica dell'evento, delle sue cause e dei possibili effetti avversi;

III. Reazione alla violazione:
    6. Individuazione delle misure di reazione (contenimento, mitigazione e prevenzione) e loro attuazione;
    7. Accertamento del rischio residuo

IV. Eventuale notifica all'Autorità e/o comunicazione all'interessato
    8. Notificazione del data breach (Coopservice Titolare) e comunicazione all'interessato, se dovute; comunicazione al Titolare terzo (Coopservice Responsabile)

V. Verifica dell'efficacia, follow up e chiusura dell'evento
    9. verifica del livello di rischio a misure applicate e follow up.
    10. Chiusura e aggiornamento del registro. Archiviazione registrazione ed evidenze documentazione delle scelte.

***

COOSPERVICE SOC. COOP. P.A.