VERIFICATO da DPO	APPROVATO da AD

core.consulting
core.lab

POLICY PER IL TRATTAMENTO DEI DATI PERSONALI

COPIA n°	1	☒ CONTROLLATA	NON CONTROLLATA

SOMMARIO

1 Premessa

Il presente documento ha lo scopo di fornire alle persone che lavorano in Core Consulting e Core Lab le indicazioni operative per gestire, nell'ambito delle attività professionali svolte (sviluppo commerciale ed erogazione dei servizi ai clienti) i dati personali dei clienti nel rispetto delle normative vigenti e delle regole adottate da entrambe le società. Una trattazione più ampia delle modalità di trattamento dei dati personali è reperibile nel documento "GDPR1 Manuale GDPR" di cui questo documento costituisce un allegato
Per quanto attiene alle attività di business di Core Consulting o Core Lab si configurano due situazioni.
Le due società agiscono:

- come Titolari del trattamento quando promuovono azioni commerciali e di marketing su propria iniziativa.
- in veste di Responsabili esterni del trattamento, su nomina esplicita o implicita dai clienti (Titolari del Trattamento) nello svolgimento dei progetti affidati.

In veste di Titolari o di Responsabili esterni autorizzano i propri dipendenti e i propri collaboratori a partita IVA al trattamento dei dati personali necessari per lo svolgimento delle attività di business.
Le persone autorizzate/responsabili del trattamento devono garantire il rispetto delle finalità e delle modalità di trattamento definite dal Titolare/Responsabile esterno.
La presente policy stabilisce le regole che tutte le persone di Core Consulting e Core Lab devono rispettare relativamente al trattamento dei dati personali.
Nota: nel seguito si intende con "servizi erogati in modalità standard" le tipologie di servizi (formazione, coaching, sviluppo, consulenza) erogati come descritto nel documento "GDPR1-Manuale GDPR"..

2 I ruoli che agiscono per l'applicazione del GDPR

I ruoli che agiscono in veste di autorizzati/responsabili del trattamento hanno quindi la responsabilità di attuare le misure descritte nel seguito.
In funzione del loro effettivo coinvolgimento nei progetti, possono essere

- **Client leader**, sempre presente e attivo in particolare nella relazione con il committente e che gestisce le attività precontrattuali finalizzate alla definizione degli aspetti inerenti alla privacy. Il client leader ha la responsabilità di verificare l'adeguatezza dell'informativa privacy e della eventuale richiesta di consenso al trattamento in funzione delle specifiche finalità e modalità di trattamento previste per la realizzazione dei progetti acquisiti
- **Capo progetto**, sempre presente per l'erogazione di ogni servizio fornito da Core Consulting e/o da Core Lab, attivo nella relazione con i referenti del progetto presso il cliente. Il capo progetto assicura la gestione del ciclo di vita dei dati personali trattati secondo gli accordi stipulati con il cliente e nel rispetto della policy del gruppo Core. In particolare, il capo progetto compila il registro dei trattamenti (vedi capitolo sulla compilazione del registro dei trattamenti) e cura la messa in atto delle misure di fine vita dei dati personali (cancellazione, anonimizzazione, pseudonimizzazione), sfruttando a tale scopo, se esistenti, gli automatismi predisposti dal System Admin.
- **Membri del team** di progetto, informati e coinvolti dal capo Progetto, evidenziati nel registro dei trattamenti, che trattano i dati secondo istruzioni descritte in questo documento o in base a specifiche istruzioni concordate con il cliente in fase contrattuale.
- **Responsabile help-desk**, se per l'erogazione dei servizi sono utilizzate piattaforme proprietarie (Skillup, Playground, Eventapp e Skillkeeper). Le persone che svolgono questo ruolo sono parte del team di progetto e soggette quindi al rispetto delle indicazioni inerenti al trattamento dei dati personali
- **Tutor**, per i servizi di formazione, in presenza o a distanza, che lo prevedono. Le persone che svolgono questo ruolo sono parte del team di progetto e soggette quindi al rispetto delle indicazioni inerenti al trattamento dei dati personali
- **Data Protection Office (DPO)**: funzione di consulenza Core Consulting/Core Lab per la piena adozione del GDPR.
- **Team Privacy**: composto da: DPO, dal responsabile ICT qualità Ambiente e Sicurezza, dai System Admin
- **System Admin:** si occupa di configurare monitorare le componenti infrastrutturali che consentono alle piattaforme il corretto funzionamento. Questa figura professionale non è un membro del team di progetto. Vede i dati personali in forma anonima (criptati) e non è autorizzato a decriptarli.

- **Responsabili Service Line:** predispongono, in accordo con il DPO, le informative privacy standard da utilizzate per l'erogazione dei servizi che afferiscono alla Service Line presidiate
- **Amministratore applicativo delle piattaforme** (se per l'erogazione dei servizi sono utilizzate piattaforme proprietarie). E' a tutti gli effetti un membro del team di progetto, incaricato di configurare e gestire le piattaforme utilizzate; carica le anagrafiche a sistema, distribuisce le credenziali di accesso, scarica i report. Per alcuni progetti questo ruolo può essere ricoperto da più di una persona. Le persone che svolgono questo ruolo devono essere informate dal capo progetto ed essere evidenziate in modo specifico nel registro dei trattamenti (vedi capitolo sulla compilazione del registro dei trattamenti)

AMMINISTRATORI DI PIATTAFORMA	SkillupP	Playground	Skillkeeper	Event app
Roberta Bortolla	X			
Domenico Delcuratolo	X			
Paolo Tripodi	X			
Ugo Capra		X		
Daniele Mela		X		
Martina Simonetti			X	
Enrico Bossi				X

3 Privacy by Design e Privacy by Default

Il principio di Privacy by Design impone di integrare la protezione dei dati fin dalla progettazione dei servizi e dei sistemi. e impone che vengano trattati solo i dati necessari per la finalità progettuale.
L'approccio si traduce in attività e punti di attenzione:

in fase di offerta e progettazione:

- Definire fin dall'avvio del progetto quali categorie di dati personali sono strettamente necessarie, evitando la raccolta di dati in eccesso (minimizzazione).
- Valutare se sia possibile utilizzare dati aggregati, pseudonimizzati o anonimi in luogo di dati personali identificativi.

nel caso di configurazione delle piattaforme:

- Gli Amministratori applicativi configurano le piattaforme in modo da rendere visibili a ciascun utente solo i dati necessari al proprio ruolo (principio del minimo privilegio).
- Le impostazioni di default delle piattaforme devono garantire il livello più elevato di protezione dei dati senza richiedere interventi attivi dell'utente.

nel caso di sviluppo software:

- I requisiti di protezione dei dati devono essere inclusi nelle specifiche funzionali del progetto.
- I dati di test non devono contenere dati personali reali, salvo espressa necessità documentata e adeguatamente protetta.

in fase di erogazione dei servizi:

- I documenti di lavoro che contengono dati personali devono riportare solo i dati strettamente necessari; ove possibile si utilizzano iniziali, codici o dati aggregati.
- La condivisione di file contenenti dati personali avviene esclusivamente tramite i canali autorizzati descritti nel capitolo 5.2.

4 Adempimenti per l'applicazione del GDPR

4.1 Informativa privacy e consenso al trattamento

E' sempre obbligatorio consegnare a clienti e prospect l'informativa privacy con modalità che garantiscano la tracciabilità della consegna.
Ciò riguarda anche i contatti con i prospect per scopi commerciali.
I responsabili delle service line e i product manager hanno la responsabilità di definire le informative standard per i prodotti/servizi di cui si occupano e le relative richieste di consenso al trattamento laddove necessarie.
I capi progetto hanno la responsabilità di aggiornare le informative nel caso i servizi erogati prevedano modalità non standard di trattamento dei dati personali.
Le informative devono obbligatoriamente descrivere i seguenti aspetti:

- Chi tratta i dati (titolare e contatti)
- Perché vengono trattati (finalità)
- Su quale base legale (consenso, contratto, obbligo di legge, ecc.)
- Quali dati sono trattati
- A chi possono essere comunicati
- Per quanto tempo sono conservati
- Quali diritti ha l'interessato
- Diritto di reclamo al Garante
- Se i dati sono obbligatori e le conseguenze del mancato conferimento
- Eventuale profilazione / decisioni automatizzate

Nelle informative si deve esplicitare, se del caso, la presenza di Core Lab come sub responsabile del trattamento.
Il consenso al trattamento va richiesto obbligatoriamente:

- per le attività di direct marketing
- in tutti i casi in cui si utilizzano dati personali particolari o modalità di trattamento ritenute rischiose (vedi tabella sinottica più avanti).

4.1.1 Informativa per le attività commerciali

I contatti con i prospect (invio di mail o telefonate) sono ammessi e non serve il consenso se:

- Il contenuto della comunicazione è professionale e gli indirizzi e-mail/ i numeri di telefono utilizzati sono aziendali
- il destinatario è un ruolo coerente con il contenuto della comunicazione (es. HR per servizi HR)
- il contenuto è strettamente pertinente all'attività svolta;
- l'impatto sulla privacy è limitato e prevedibile;
- è garantito diritto di opposizione immediato (unsubscribe).

In altri termini se sono rispettate le seguenti condizioni:

- contatti professionali
- finalità di business
- comunicazioni proporzionate e non invasive

E' sempre necessaria una Informativa privacy chiara e la possibilità di rifiutare la reiterazione del contatto
Quindi, in ogni mail (almeno nella prima) verso i prospect deve essere inserita una dicitura del tipo:

"Ai sensi del Regolamento (UE) 2016/679 ("GDPR"), [Core Consulting o Core Lab] tratta i dati di contatto professionali del destinatario per finalità connesse alla propria attività istituzionale e di sviluppo delle relazioni professionali, sulla base del legittimo interesse del Titolare.
Il destinatario può opporsi in qualsiasi momento al ricevimento di ulteriori comunicazioni scrivendo a [mittente della mail e pc a security@coreconsulting.it].
L'informativa completa sul trattamento dei dati personali è disponibile al seguente link: [link informativa privacy per

*attività commeciali]**.***

Firma standardizzata:

- *dati del mittente della mail*
- *dati del titolare"*

4.1.2 Consenso per le attività di direct marketing

Nel caso di iniziative di direct marketing, è necessario che oltre all'informativa sia presente in modo esplicito e distinto dall'informativa, anche la richiesta di consenso al trattamento, tipo la seguente, fornita a mero scopo esemplificativo. Il testo della richiesta di consenso al trattamento, dovrà essere definita ad hoc per la specifica attività di direct marketing che si intende realizzare:

"Autorizzo [Core Consulting S.r.l. / Core Lab S.r.l.], in qualità di Titolare del trattamento, al trattamento dei miei dati personali (nome, cognome, indirizzo e-mail, ruolo professionale) per l'invio di comunicazioni commerciali, newsletter e proposte di servizi, mediante posta elettronica o altri canali digitali.
Ho letto l'informativa completa sul trattamento dei dati disponibile al seguente link: [link informativa]. Sono consapevole che il conferimento del consenso è facoltativo e non condiziona l'erogazione di altri servizi, e che posso revocare il mio consenso in qualsiasi momento scrivendo a security@coreconsulting.it o cliccando sul link di cancellazione presente in ogni comunicazione.
□ Acconsento al trattamento dei miei dati per finalità di marketing diretto (barrare la casella per esprimere il consenso)"

4.2 Data protection impact assessment (DPIA)

Per le tipologie di servizio erogate (Formazione, Coaching, Sviluppo, Consulenza) sono state sviluppate DPIA standard, riferite a modalità consuete di erogazione descritte nel documento "-GDPR5-DPIA servizi standard". La descrizione dei servizi presente nel manuale "GDPR1-Manuale GDPR" è articolata esattamente come gli item che compongono la DPIA. Se per l'erogazione dei servizi si utilizzano modalità diverse da quelle descritte, è necessario adeguare la DPIA standard per analizzare il livello di rischio per la protezione dei dati associato a tali modalità. A tale scopo è necessario considerare tutti gli item in cui si articola una DPIA, descritti nella tabella seguente.

Sezione	Elementi da analizzare
Descrizione sistematica del trattamento	Finalità del trattamento
	Tipologia di dati
	Interessati
	Flussi e strumenti di trattamento
Valutazione di necessità e proporzionalità	Pertinenza dei dati
	Minimizzazione
	Basi giuridiche
	Rispetto dei diritti degli interessati
Analisi dei rischi	Rischi per i diritti e le libertà degli interessati
	Probabilità e gravità degli impatti
Misure di mitigazione	Misure tecniche e organizzative
	Garanzie, sicurezza, privacy by design / by default
Valutazione del rischio residuo	Accettabilità del rischio
	Eventuale consultazione preventiva del Garante
Documentazione e riesame	Formalizzazione della DPIA
	Aggiornamenti periodici in caso di cambiamenti

4.3 Compilazione del registro dei trattamenti

Il trattamento dei dati personali delle persone del cliente che fruiscono o collaborano alla realizzazione dei servizi erogati da Core Consulting e Core Lab, deve essere tracciato, utilizzando l'apposito registro dei trattamenti "GDPR6-Modulo registro trattamento dati personali" Tale modulo consiste in un foglio excel reperibile nella cartella "GDPR" del DB CORECONSULTING.
La compilazione del registro dei trattamenti, anche in forma di bozza provvisoria, quando richiesto, è condizione necessaria e preventiva per la compilazione della documentazione inerente alla nomina a responsabile esterno del trattamento.
Responsabile della compilazione del registro è il project manager incaricato della conduzione del progetto.
La compilazione è opportuna per ogni progetto ed è obbligatoria (come indicato nella tabella che più avanti descrive gli adempimenti):

- nel caso di nomina di Core Consulting o Core Lab a responsabile esterno del trattamento
- per i progetti che trattano dati personali più ampi dei soli dati di contatto
- per le iniziative di direct marketing
- nel caso si preveda la profilazione delle competenze delle persone
- nel caso si utilizzino strumenti di AI per l'erogazione dei servizi
- nel caso di trattamento di dati particolari. Per la definizione di "dati particolari" consultare il manuale GDPR (documento "GDPR1 Manuale GDPR)

Il capo progetto, compila il registro dei trattamenti, considerando le caratteristiche del servizio da erogare, le modalità di trattamento dei dati personali, avendo come riferimento il manuale GDPR (documento "GDPR1 Manuale GDPR) che riporta per ogni tipologia di servizio erogato (Formazione, Coaching, Sviluppo, Consulenza) specifiche indicazioni.
Nel caso il trattamento che il progetto richiede, si differenzi da quelli descritti nel manuale, il capo progetto dovrà specificare quali siano le peculiarità e nello stesso tempo, se e quali misure tecniche particolari sono messe in atto per gestire tali peculiarità.
Il capo progetto dovrà indicare i nominativi dei membri del team che avranno accesso ai dati personali e dovrà informare per iscritto gli stessi membri del team sulle corrette modalità di gestione di tali dati, secondo la presente policy e/o in base a specifiche richieste del Titolare del trattamento (il Cliente) e/o a necessità particolari inerenti alla gestione del progetto da realizzare.

4.4 Accesso ai dati personali e loro trattamento

Secondo il GDPR, possono avere accesso ai dati personali esclusivamente i soggetti:

1. formalmente autorizzati,
2. coinvolti nelle attività specifiche del servizio,
3. nei limiti delle finalità dichiarate,

limitatamente ai dati strettamente necessari allo svolgimento del proprio ruolo.
Anche i dati di contatto devono essere gestiti secondo questi principi e per tale scopo i dipendenti e i collaboratori a partita IVA sono esplicitamente autorizzati da Core Consulting o Core Lab. Nello specifico i client leader sono autorizzati a trattare i dati di contatto dei clienti ad essi affidati, così come i capi progetto o chi ritiene di poter agire commercialmente previo incarico dell'AD (in quanto rappresentante dell'azienda Titolare del trattamento dei dati personali di contatto con i prospect)
In alcuni casi (cfr. tabella precedente) è necessario gestire l'accesso ai dati in modo più restrittivo. In tali casi i dati personali devono essere visibili e trattabili dalle sole persone che fanno parte dei team di progetto deputati alla realizzazione degli specifici progetti. I file archiviati sul DB CORECONSULTING sono accessibili da tutte le persone dotate di un account Core Consulting o Core Lab e quindi i file che contengono tali dati personali non possono risiedere sul DB CORECONSULTING.
I dati personali, devono invece essere segregati in cartelle riservate ai i soli membri dei team di progetto.
La segregazione dei dati personali, nel caso serva, avviene nel modo seguente:

1. Il capo progetto compila un apposito form, reperibile sul DB CORECONSULTING nella cartella GDPR, per la richiesta di creazione di una cartella per la segregazione dei dati personali trattati nello specifico progetto.
2. La compilazione del form produce la creazione di una cartella che risiede sul One Drive dell'account

"trattamentodatipersonali@coreconsulting.it" (account la cui gestione e riservata ai membri del team privacy)

3. Il capo progetto riceve il link privato alla cartella di segregazione creata . Con link privato si intende un link che può essere utilizzato solo dal capo progetto destinatario.
4. Il capo progetto, sotto la propria responsabilità condivide la cartella di segregazione dei dati personali da trattare, con i membri del team di progetto

Nota: i file che non contengono dati personali da segregare vanno gestiti sul DB CORECONSULTING

4.5 Scambio dati personali con i clienti

Lo scambio di dati personali tra Core Consulting o Core Lab e i clienti deve avvenire usando strumenti in grado di garantire la massima protezione dei dati.
La soluzione più efficace al momento è quella di creare un'apposita cartella temporanea nella quale scaricare/caricare file che devono essere trasferiti da e verso il cliente
La cartella temporanea di scambio dati personali deve essere creata dal capo progetto come sotto cartella della cartella nella quale risiedono i file che contengono dati personali da trattare (vedi capitolo precedente):

- la cartella per lo scambio dati deve essere una cartella diversa da quella che serve al team di progetto per trattare i dati personali necessari alla realizzazione del progetto perché è necessario che la cartella per lo scambio dei dati con il cliente contenga file per il solo tempo necessario allo scambio.
- la cartella per lo scambio dati deve essere protetta da password
- Il capo progetto condividerà tale cartella con uno specifico referente del cliente abilitato allo scambio di file contenenti dati personali. La condivisione deve avvenire mediante le funzionalità di one drive. Nel caso tali funzionalità non possano essere utilizzate perché incompatibili con i vincoli tecnologici del cliente, una possibile modalità alternativa di condivisione, consiste nell'inviare via mail al referente il link della cartella e su un canale diverso, ad esempio mediante sms, la password di accesso. In questo caso le password utilizzate devono soddisfare i seguenti requisiti::
    - diversa da username (controllo sistema)
    - almeno 8 caratteri (controllo sistema)
    - almeno 3 delle seguenti categorie di caratteri (maiuscole, minuscole, numerici, speciali) (controllo sistema)
    - non facile da indovinare, non riferibile alla persona, non parola di vocabolario pubblico delle parole note, etc.

  Nel caso anche questo sistema non fosse utilizzabile è necessario valutare con il team privacy altre soluzioni.

4.6 Conservazione dei dati

In fase di offerta o contrattualizzazione del servizio il client leader deve esplicitare/concordare con il cliente la modalità di trattamento dei dati personali a fine progetto evidenziando che in assenza di accordi specifici i dati personali saranno cancellati/anonimizzati.
Al termine dei progetti, i file contenenti dati personali dei clienti, utilizzati durante il progetto e conservati nella cartella di segregazione definita nel capito 4.1, ed in particolare i file classificati come deliverable, previa cancellazione/anonimizzazione o pseudonimizzazione dei dati personali in essi contenuti, devono alimentare la base di conoscenza di Core Consulting e Core Lab ed essere quindi archiviati nel DB CORECONSULTING, secondo le regole di Knowledge management definite.
E' compito del Capo Progetto, cancellare o anonimizzare (trattamento di default) i dati personali contenuti nei file da conservare. Parimenti, in caso di accordi diversi stipulati con il cliente, su tempi e modalità di conservazione dei dati, il capo progetto deve provvedere alla loro attuazione, con l'eventuale supporto tecnico degli Amministratori di piattaforma e/o del System Admin.
Nonostante il trattamento finale (cancellazione / anonimizzazione) dei dati al termine del progetto sia esplicitato nella documentazione contrattuale, data l'irreversibilità del trattamento, è buona norma informarne il cliente prima di attuarlo.
Una volta attuato il trattamento finale dei dati personali e dopo aver archiviato i file sul DB CORECONSULTING, Il capo progetto richiede al Team Privacy la cancellazione della cartella di segregazione dei dati e della sottocartella utilizzata per lo scambio dati con i cliente (cfr. capitolo 4.1). La richiesta di cancellazione della cartella di segregazione dei dati avviene

utilizzando l'apposito form reperibile nella cartella GDPR del DB CORECONSULTING. Si sottolinea che è responsabilità del capo progetto provvedere alla corretta preparazione e conservazione dei file al termine del progetto. Eventuali carenze o errori nel trattamento dei file contenti i dati personali non sono in alcun modo imputabili al team Privacy che svolge solo attività di consulenza e supporto per il pieno rispetto del GDPR.
Si precisa che con "conclusione del progetto", nel caso tutte le attività siano effettivamente completate, si intende la data di pagamento della fattura a saldo per il servizio erogato (che avviene di norma 60 gg. dopo l'emissione della fattura). Diversamente, ovvero nel caso di pagamenti anticipati rispetto al termine reale delle attività, la data di conclusione del progetto è a 60 gg. dalla data di conclusione effettiva delle attività

4.7 Sinottico degli adempimenti

La seguente tabella riassume gli adempimenti correlati alle attività caratteristiche di Core Consulting e Core Lab.

SERVIZI / ATTIVITA'	Dati accessibili ai soggetti autorizzati coinvolti nelle attività		Adempimenti			
	Dati che non richiedono la segregazione	Dati che richiedono la segregazione	Informativa	Consenso	DPIA (*)	Registro dei trattamenti
Attività commerciali	• Nome • Cognome • Indirizzo e-mail • Ruolo professionale • Numero di telefono		SI, sviluppata centralmente dal team Privacy	NO	NO	SI, compilato centralmente una tantum e aggiornato, se del caso, dal team Privacy
Marketing (es. direct mail, newsletter, …)		Tutti i dati personali, inclusi i dati di contatto nei limiti della finalità perseguita	SI, redatta dal responsabile dell'iniziativa e supervisionata dal DPO	SI	SI, sviluppata dal responsabile dell'iniziativa	SI, compilato dal capo progetto dell'iniziativa
Formazione, Coaching e Consulenza	• Nome • Cognome • Indirizzo e-mail • Ruolo professionale • Numero di telefono	• Anni di anzianità aziendale • Immagine personale • Competenze • Qualifica contrattuale • Età • Codice fiscale • Indirizzo di residenza • Retribuzione • Altri dati diversi dai dati di contatto	SI, aggiornata dal client leader sulla base di quella standard prevista per il servizio	NO (tranne che per il trattamento dell'immagine personale o di dati particolari)	SI, sviluppata dal client leader se il servizio è erogato con modalità non standard o utilizza strumenti di AI	SI, se sono presenti dati da segregare, compilato dal capo progetto
Sviluppo		Tutti i dati personali, inclusi i dati di contatto	SI, aggiornata dal client leader sulla base di quella standard prevista per il servizio	SI	SI, sviluppata dal client leader se il servizio è erogato con modalità non standard o utilizza strumenti di AI	SI, compilato dal capo progetto
Ogni servizio nel caso di nomina esplicita di Core Consulting o Core Lab a Responsabile esterno del trattamento		Tutti i dati personali, inclusi i dati di contatto	SI, redatta dal client leader e supervisionata dal DPO, sulla base della nomina ricevuta	NO (tranne che per i servizi di Sviluppo e per il trattamento dell'immagine personale o di dati particolari)	Si, sviluppata dal client leader se il servizio è erogato con modalità non standard	SI, compilato dal capo progetto

(*) nel caso di erogazione dei servizi con modalità standard, ovvero quelle descritte nel documento GDPR1-Manuale GDPR è possibile utilizzare le DPIA standard disponibili nel documento GDPR5-DPIA servizi Standard

5 Reperimento e archiviazione della documentazione inerente al GDPR

TIPOLOGIA	DOCUMENTO	REPERIBILE	DA ARCHIVIARE
Manuali e riferimenti operativi	GDPR1-Manuale GDPR	In DB CORECONSULTING/COMUNICAZIONI CORE/GDPR	
	GDPR2-Tecnologie e GDPR		
	GDPR3-Misure di sicurezza e GDPR		
	GDPR4-Policy GDPR		
	GDPR 5-DPIA servizi standard		
Modulistica	GDPR6-Modulo registro trattamento dati personali	In DB CORECONSULTING/COMUNICAZIONI CORE/GDPR/Modulistica	
	GDPR7-Modulo creazione cartella dati personali		
	GDPR7-Modulo cancellazione cartella dati personali		
Documentazione contrattuale	Check list misure di sicurezza e privacy		Presso l'amministrazione, insieme all'ordine
	Nomina a responsabile esterno		
Documentazione di progetto	Informativa privacy		In DB CORECONSULTING/CLIENTI/<nome cliente>/<anno_Cliente_Nome progetto>/documentazione cliente
	Registro dei trattamenti		
	DPIA		
	Consensi al trattamento		In Skillup i consensi sono conservati in piattaforma. Negli altri casi, • se in forma digitalizzata, devono essere archiviati nella cartella di segregazione dei dati personali • se in forma cartacea, devono essere archiviati in armadi accessibili al Capo Progetto e distrutti con gli stessi tempi con i quali si cancellano le cartelle di segregazione dei dati

6 Responsabilità e attività dei ruoli

6.1 Client leader

FASE	ATTIVITA'
Contatto commerciale / marketing	• Fornire l'informativa sul trattamento dei dati personali o il link a cui può essere reperita • Richiedere il consenso se si sta conducendo un'attività di marketing diretto
Offerta	• Esplicitare che in base all'approccio Privacy by design e privacy by default" si richiede di fornire solo i dati personali indispensabili per la conduzione del progetto e che in tutte le fasi progettuali saranno applicate procedure e misure tecniche per la compliance con il GDPR • Evidenziare che, a meno di diverse indicazioni del cliente, al termine del progetto i dati personali trattati saranno cancellati o resi anonimi e non saranno quindi più disponibili
Contratto	• Valutare attentamente i contenuti della (eventuale) nomina formale a responsabile esterno del trattamento che il cliente vuole conferire a Core Consulting o Core Lab, considerandone la pregnanza rispetto alle effettive attività di trattamento dei dati personali necessarie per lo svolgimento del progetto e la compliance con il GDPR. Approfondire e discutere con il cliente la reale necessità dei requisiti presenti nella nomina a responsabile esterno. • Compilare la documentazione (check list privacy, misure tecniche, documento di nomina) inviata dal cliente per la nomina a responsabile esterno del trattamento e previa attenta verifica delle possibilità di rispettare le clausole richieste dal cliente, prima di farla sottoscrivere all'AD
Avvio del progetto	• Controllare che sia predisposto dal Capo Progetto il registro dei trattamenti e che i membri del team siano stati edotti in forma scritta sulle corrette modalità di trattamento dei dati personali
Realizzazione del progetto	• Verificare che il capo progetto applichi la policy GDPR in tutti i suoi aspetti ed in particolare per ciò che attiene alla segregazione e alle modalità di scambio dei dati personali
Chiusura del progetto	• Verificare che il capo progetto attui il trattamento finale dei dati personali previsto per default o dagli accordi specifici stipulati con il cliente. • Verificare che i file da conservare, dopo essere stati resi anonimi, siano stati archiviati sul DB CORECONSULTING

6.2 Capo Progetto

FASE	ATTIVITA'
Avvio del progetto	• Richiedere al Team Privacy la creazione della cartella per la segregazione dei dati personali che non deve essere condivisa con persone esterne a Core Consulting o Core Lab • Creare la cartella per lo scambio dei dati da e verso il cliente (da condividere solo con i referenti del progetto presso il cliente) • Richiedere e utilizzare soltanto i dati previsti dall'informativa e necessari alla normale attività lavorativa e verificare che il personale del cliente coinvolto nel progetto non fornisca inavvertitamente dati particolari o dati non essenziali allo svolgimento del progetto • Compilare il registro dei trattamenti • Informare, in forma scritta, i membri del team sulle regole da osservare per il trattamento dei dati personali (condividendo anche la cartella per la segregazione dei dati personali) • Fornire alle persone del cliente coinvolte nel progetto l'informativa sul trattamento dei dati personali e richiedere, laddove necessario, il consenso al trattamento
Realizzazione del progetto	• Acquisire dal cliente solo i dati personali strettamente necessari allo svolgimento del progetto • Verificare che i membri del team applichino la policy GDPR in tutti i suoi aspetti ed in particolare per ciò che attiene alla segregazione e alle modalità di scambio dei dati personali • Effettuare una revisione periodica degli accessi, verificare l'elenco degli utenti con accesso

	attivo. Rimuovere l'accesso a coloro che non sono più coinvolti • Gestire il trasferimento al cliente dei file contenenti dati personali • Segnalare immediatamente al Team Privacy qualsiasi anomalia riscontrata inerente la protezione dei dati: accessi non autorizzati, invio errato di file, sospetti data breach, ...
Chiusura del progetto	• Attuare il trattamento finale dei dati personali previsto per default o dagli accordi specifici stipulati con il cliente. • Archiviare sul DB CORECONSULTING i file da conservare, emendati dei dati personali • Richiedere al Team Privacy la cancellazione della cartella di segregazione dei dati e di scambio dati con il cliente • Fornire al System Admin indicazioni per la chiusura di servizi che abbiano utilizzato piattaforme. Le indicazioni devono comprendere: o Eventuale necessità di estrazione dati qualora non siano sufficienti i dati sino a quel momento scaricati o Indicazioni su pseudonimizzazione, anonimizzazione o cancellazione completa e definitiva dei dati personali o Eliminazione completa e definitiva di ogni eventuale mail utilizzata come contatto help-desk o altro (indicarne il riferimento) o Eliminazione completa e disdetta di domini e certificati associati al servizio (indicare s ea cura nostra o a cura cliente) • Assicurarsi che entro 10 gg. lavorativi dalla richiesta effettuata, tutti i dati personali siano stati trattati come da indicazioni fornite

6.3 Membro del team:

FASE	ATTIVITA'
Avvio del progetto	• Conoscere l'informativa privacy fornita al cliente • Conoscere e rispettare l'impegno di riservatezza • Comprendere le regole di trattamento dei dati personali comunicate dal Capo Progetto
Realizzazione del progetto	• Rispettare le regole condivise e più in generale la policy GDPR • Segnalare tempestivamente al capo progetto eventuali anomalie riscontrate nella gestione dei dai personali
Chiusura del progetto	• Garantire che i file contenenti dati personali trattati siano pronti per essere trasferiti dal Capo Progetto sul DB CORECONSULTING

7 Norme di sicurezza informatica per il trattamento dei dati personali

- Non sincronizzare o salvare sul proprio PC o su dispositivi mobili file che contengono dati personali utilizzati nello svolgimento del progetto
- Non archiviare nel DB CORECONSULTING dati personali oggetto di trattamento
- Utilizzare solo le proprie utenze di accesso e non comunicarle a terzi per nessuna ragione
- Non fornire dati personali in modi estemporanei, ad esempio telefonicamente o su chiavetta usb
- Utilizzare sempre password di protezione degli accessi ai dati personali. Nel caso di dati personali trasmessi via mail, fornire la password di decriptazione o di accesso ai link per il download dei dati, mediante canali diversi da quelli utilizzati per trametterе i dati/i link