CoreTech
The #1 New Generation Provider
Viale Ortles 13, 20139 Milano (MI) - Italy PEC: coretech@pec.coretech.it
REA MI - 1703914 - Codice fiscale e Partita IVA 03815480961 - Capitale Sociale 10.000,00 Euro

DPA – DATA PROCESSING AGREEMENT:
ACCORDO RELATIVO ALLA NOMINA DEL RESPONSABILE DEL TRATTAMENTO EX ART. 28 GDPR

SOMMARIO

SEZIONE I
DISPOSIZIONI GENERALI

art. 1 Premesse

1.01 Quali parti integranti del presente accordo la CORETECH ed il CLIENTE convengono sulle seguenti premesse di fatto:

(a) come indicato nel contratto di servizi, la CORETECH fornisce servizi informatici come ivi descritti (IaaS, SaaS, servizi di manutenzione correlati) che comportano la necessità di accedere anche potenzialmente ai dati del CLIENTE, quale presupposto tecnico per poter erogare i servizi oppure fornire la relativa assistenza;

(b) questo comporta quindi che la CORETECH svolga trattamenti sui dati personali gestiti dal CLIENTE tramite i servizi forniti, operando questi trattamenti esclusivamente per conto di quest'ultimo;

(c) i dati personali gestiti dal CLIENTE tramite i servizi in parola possono essere di ogni tipo, comuni, particolari o anche relativi a condanne penali o reati, essendo solo il CLIENTE a decidere come utilizzare i servizi e quindi quali dati personali inserire e quali trattamenti effettuare, limitandosi CORETECH a fornire solo i servizi informatici;

(d) il CLIENTE inoltre può effettuare il trattamento dei dati personali decidendo le finalità e i mezzi di trattamento oppure può a sua volta trattare i dati per conto di altro soggetto, da cui riceve le istruzioni circa il trattamento di tali dati personali;

(e) il CLIENTE quindi può essere sia direttamente un titolare (o contitolare) del trattamento oppure un responsabile o sub-responsabile del trattamento a seconda del tipo di servizio che a sua volta il CLIENTE fornisce a terzi;

(f) date queste premesse, si rende necessario regolare le modalità con cui CORETECH gestisce i trattamenti dei dati personali per conto del CLIENTE, al fine di assicurare che il trattamento rispetti la disciplina sulla privacy e garantisca la tutela dei diritti e libertà degli interessati;

(g) il presente accordo intende disciplinare gli obblighi e i diritti spettanti alle parti, CORETECH e il CLIENTE, relativamente al rispetto degli adempimenti previsti dalla normativa privacy, in particolare il regolamento (UE) 2016/679 (d'ora innanzi GDPR) e il codice della privacy di cui al D.lgs. 30.06.2003 n. 196, come modificato D.lgs. 10.08.2018 n. 101 ed eventuali successive modificazioni o integrazioni nonché la relativa disciplina regolamentare da essa derivante;

(h) CORETECH ha adottato le misure tecniche ed organizzative al fine di garantire che i servizi offerti ai propri clienti abbiano un'adeguata protezione, secondo standard tecnici di mercato, al fine di assicurare una efficiente tutela dei diritti e delle libertà degli interessati in relazione ai loro dati personali.

1.02 Il presente accordo deve intendersi come parte integrante del contratto di fornitura di servizi CORETECH, avendo ad oggetto la disciplina dei conseguenti adempimenti di cui all'art. 28 GDPR, ripartendoli tra CORETECH e il CLIENTE secondo il principio di responsabilità condivisa come di seguito precisato.

art. 2 Definizioni

2.01 Al fine dell'applicazione ed interpretazione del presente accordo i termini e le espressioni utilizzati dovranno intendersi secondo quanto di seguito indicato:

(a) Si terrà conto delle definizioni che sono state indicate nel contratto di servizi concluso tra CORETECH e il CLIENTE;

(b) Si terrà contro altresì delle definizioni normative previste dalla disciplina sulla privacy, tra cui in primo luogo quanto stabilito dall'art. 4 § 1 GDPR nonché quanto consolidato dalla prassi applicativa proposta dagli organi europei competenti in materia e dall'Autorità Garante per la protezione dei dati personali italiana, oltre alla giurisprudenza europea e italiana pertinente;

(c) Per comodità espositiva si considera "responsabile del trattamento" colui che tratta di dati per conto di un titolare del trattamento, mentre si considera "sub-responsabile" colui che tratta dati per conto di un responsabile del trattamento o un altro sub-responsabile del trattamento;

(d) Nel corso del presente accordo per semplice comodità espositiva, CORETECH è indicata quale

responsabile del trattamento, anche nel caso sia qualificabile come sub-responsabile in relazione al ruolo rivestito dal CLIENTE.

art. 3 Nomina di CORETECH quale responsabile del trattamento

3.01 Il CLIENTE nomina CORETECH responsabile del trattamento dei dati personali i quali vengono trattati tramite i servizi informatici, oggetto del contratto di fornitura concluso con la seconda, autorizzando quest'ultima al trattamento, per conto del primo, dei relativi dati personali e solo in quanto necessario per l'erogazione dei servizi informatici stessi, nel rispetto dei termini contrattuali di fornitura e secondo quanto stabilito nel presente accordo.

3.02 In relazione alla nomina si concorda che:

(a) Le finalità del trattamento dei dati personali trasmessi dal CLIENTE sono esclusivamente quelle di erogare i servizi informatici di cui al precedente comma e sono effettuate per conto del CLIENTE da parte di CORETECH, quale responsabile del trattamento, secondo le indicazioni del presente accordo od anche su specifica istruzione scritta di quest'ultimo, sempre se conforme alla disciplina sulla privacy e nel rispetto dei termini contrattuali del servizio;

(b) Nell'ambito dei trattamenti consentiti al responsabile del trattamento di cui alla lettera precedente, è compresa anche l'attività di assistenza tecnica, l'aggiornamento e la manutenzione dei sistemi informatici richiesta dal CLIENTE, se del caso anche in modalità "*on premise*", e possono consistere in tutte le relative operazioni di supporto e quindi a titolo esemplificativo:

- attività di migrazione dati finalizzata all'installazione ed al collaudo di software o servizi informatici;
- servizi di assistenza e aggiornamento che comportano (ancorché occasionalmente) l'accesso remoto ai dati del CLIENTE (es. tramite strumenti di accesso remoto, per es. TeamViewer, VPN, etc.);
- analisi di dati (DB, videate, esportazioni di dati, etc.) del CLIENTE per verificare problematiche di carattere tecnico e svolgere attività di manutenzione o supporto tecnico;

(c) Il responsabile del trattamento potrà effettuare i trattamenti in modalità automatizzata e/o cartacea sempre in quanto necessario per le finalità innanzi indicate;

(d) Il CLIENTE decide la tipologia di dati personali oggetto del trattamento tramite i servizi informatici forniti dal responsabile del trattamento, i quali possono essere dati personali comuni, di categoria particolare o relativi a condanne o reati;

(e) La categoria di interessati si riferisce a persone fisiche come clienti, fornitori o dipendenti del CLIENTE, dipendendo dal tipo di attività o servizi offerti a sua volta da quest'ultimo a terzi, direttamente o indirettamente;

(f) La durata del trattamento è limitata alla durata del servizio come descritto nelle condizioni generali di fornitura ed al termine i dati personali saranno cancellati secondo quanto contrattualmente stabilito, salvo diversa istruzione scritta dal CLIENTE, sempre se conforme alla disciplina sulla privacy e nel rispetto dei termini contrattuali del servizio. Resta salva l'ipotesi prevista dall'art. 28 § 3 lett. g) GDPR relativa al caso in cui il diritto dell'Unione Europea o il diritto italiano preveda la conservazione dei dati;

(g) Il CLIENTE dichiara e garantisce di avere tutti i poteri necessari per effettuare la nomina del responsabile in relazione ai dati personali che quest'ultimo tratterà per suo conto, nel rispetto della normativa sulla privacy.

art. 4 Posizione del CLIENTE rispetto ai dati personali oggetto del trattamento

4.01 Le parti si danno atto che il CLIENTE può assumere diverse posizioni in relazione alla disciplina sulla privacy, potendo essere titolare (o contitolare) del trattamento per i dati personali per i quali decide le finalità ed i mezzi di trattamento oppure se tratta i dati personali su istruzione e per conto di altri, responsabile del trattamento o sub-responsabile del trattamento a seconda dei casi.

4.02 Nel caso in cui il CLIENTE svolga le operazioni di trattamento per conto di un titolare o un responsabile del trattamento o un sub-responsabile del trattamento, il CLIENTE garantisce che il presente accordo è conforme alle istruzioni ricevute ed ai poteri conferiti, avendo verificato la regolarità della sua posizione prima di sottoscrivere le condizioni di fornitura di CORETECH e il presente accordo.

4.03 Nel caso previsto dai commi precedenti, CORETECH assumerà il ruolo di responsabile del trattamento o sub-responsabile a seconda del ruolo rivestito dal CLIENTE.

4.04 All'atto della sottoscrizione del contratto di fornitura dei servizi offerti da CORETECH, il CLIENTE dovrà specificare nel modulo d'ordine il proprio ruolo rispetto ai dati personali che verranno trattati con i servizi ordinati ed in mancanza di indicazione si intenderà che questi assuma il ruolo di titolare del trattamento.

4.05 Se nel corso del contratto di fornitura, il ruolo del CLIENTE cambia, questi è tenuto a comunicarlo al responsabile del trattamento, con le modalità ivi previste.

4.06 CORETECH compilerà il registro del responsabile del trattamento ex art. 30 co. 2 GDPR, indicando il ruolo del CLIENTE, rispetto ai dati personali oggetto del contratto di fornitura, secondo quanto da quest'ultimo dichiarato come innanzi indicato.

art. 5 Istruzioni del CLIENTE e limiti

5.01 Nell'ambito dell'esecuzione del presente accordo, CORETECH, quale responsabile del trattamento si adeguerà alle istruzioni del CLIENTE, in relazione ai dati personali oggetto di trattamento, salvo che le operazioni richieste con le istruzioni non siano previste dal presente accordo o comportino variazioni di risorse informatiche e organizzative non comprese nel contratto di fornitura dei servizi.

5.02 In quest'ultima ipotesi, CORETECH valuterà la fattibilità delle istruzioni e, se fattibile, concorderà con il CLIENTE le suddette variazioni e costi relativi. In mancanza di accordo, le istruzioni non saranno attuate, valendo quanto disciplinato dal presente accordo.

5.03 Resta inteso che le istruzioni del CLIENTE anche rientranti nel presente accordo e comunque i trattamenti svolti quale responsabile del trattamento, saranno eseguiti sempreché non comportino, a giudizio di CORETECH, una violazione della normativa sulla privacy o di un ordine imposto da una pubblica autorità.

5.04 In quest'ultimo caso CORETECH invierà senza ritardo motivazione scritta al CLIENTE, fatto salvo i divieti previsti dalla legge.

art. 6 Nomina di altri sub-responsabili da parte di CORETECH

6.01 IL CLIENTE autorizza in via generale CORETCH, quale responsabile del trattamento, a nominare sub-responsabili del trattamento per l'esplicazione di parte dei propri compiti purché nel rispetto del contratto di fornitura e del presente accordo.

6.02 L'autorizzazione suddetta comporta il potere di aggiungere nuovi sub-responsabili o sostituirli, e modificare i relativi accordi contrattuali.

6.03 L'autorizzazione generale conferita è così disciplinata:

(a) Il soggetto nominato dovrà presentare adeguate garanzie di adeguatezza sia in relazione alla sicurezza dei trattamenti e sia in relazione alla tutela dei diritti e libertà degli interessati e comunque rispettoso degli standard di mercato di settore;

(b) I trattamenti dei dati personali svolti dal sub-responsabile saranno limitati solo a quanto necessario per la fornitura di servizi subappaltati e in quanto rilevanti e utili per l'esplicazione di una parte dei servizi oggetto del contratto di fornitura di CORETECH;

(c) La nomina del sub-responsabile sarà effettuata per iscritto, imponendo obblighi di tutela non inferiore a quelli previsti dal presente accordo e dall'art. 28 GDPR;

(d) Il CLIENTE sarà preventivamente avvisato per iscritto della nomina entro un termine di 30 (trenta) giorni, il quale entro il termine suddetto potrà opporsi per iscritto. Nel caso di opposizione del CLIENTE, CORETECH potrà recedere dal contratto di fornitura con preavviso di 30 giorni, senza dar corso alla nomina del sub-responsabile in relazione ai servizi oggetto di fornitura con il CLIENTE;

(e) L'elenco dei sub-responsabili nominati da CORETECH si trova nell'area riservata del CLIENTE, nell'area "*comunicazioni contrattuali*".

art. 7 Vincoli al trasferimento dei dati personali fuori dallo Spazio Economico Europeo (SEE)

7.01 Sempre nel rispetto della normativa privacy, il responsabile potrà trasferire i dati personali del CLIENTE, se possibile tecnicamente tramite sistemi di cifratura secondo standard tecnici riconosciuti a livello internazionale, anche fuori dallo Spazio Economico Europeo (SEE) o da un paese che non goda di una decisione di adeguatezza da parte della Commissione Europea ai sensi dell'art. 45 del GDPR, esclusivamente qualora nomini un sub-responsabile ai sensi del precedente art. 6 e rispettando una delle seguenti condizioni:

(a) vengano stipulate le clausole contrattuali tipo previste nella Decisione della Commissione Europea

2010/87/UE, del 5 febbraio 2010, con il sub-responsabile del trattamento nominato da CORETECH, la quale è autorizzata fin d'ora dal CLIENTE a sottoscriverle;
(b) oppure nel caso il sub-responsabile sia situato negli Stati Uniti, anche tramite applicazione del "Privacy Shield", www.privacyshield.gov, di cui alla Decisione della Commissione Europea 2016/1250/UE del 12 luglio 2016;
(c) oppure, se il sub-responsabile del trattamento sia parte di un gruppo societario in relazione a trasferimenti infragruppo, quest'ultimo abbia ottenuto l'approvazione delle BCR (norme vincolanti d'impresa).
7.02 Il responsabile del trattamento fornisce al CLIENTE le informazioni e la documentazione idonea in relazione a quanto sopra previsto.

7.03 Nel modulo d'ordine, il CLIENTE può scegliere di non applicare la presente clausola, barrando la relativa opzione e in questo caso i dati personali saranno trattati da CORETECH esclusivamente all'interno dello Spazio Economico Europeo (SEE).

7.04 Resta salvo un diverso accordo tra le parti.

art. 8 Responsabilità condivisa e obbligo di collaborazione reciproca nel rispetto della privacy

8.01 Le parti si danno atto che l'efficienza, sicurezza e conformità alla normativa sulla privacy dei servizi cloud forniti da CORETECH, sono oggetto di una responsabilità condivisa tra quest'ultima e il CLIENTE, che obbliga entrambe le parti ad attivarsi con la dovuta diligenza per la gestione dell'ambito informatico di propria competenza e sotto la propria responsabilità.

8.02 A titolo esemplificativo, al fine di far comprendere il concetto di responsabilità condivisa, è sintetizzata nella pagina web https://www.coretech.it/it/service/chi_siamo/gdpr.php (di cui è stato estratto il relativo file pdf trasmesso alle parti impronta sha256: 7A97493DB3834DE020885D4BBE413611D5B20E8545A22DBEFC3F40273A527449) la ripartizione di compiti con il CLIENTE, relativi ai servizi offerti da CORETECH. I contenuti della suddetta pagina potranno essere aggiornati nel tempo in relazione allo sviluppo tecnologico dei servizi offerti.

8.03 Ognuna delle parti si impegna inoltre a rispettare i propri obblighi derivanti dalla disciplina sulla privacy ed a collaborare secondo buona fede nell'ambito dell'applicazione del presente accordo al fine di garantire i diritti e le libertà degli interessati.

art. 9 Modalità di comunicazione tra le parti

9.01 La modalità di comunicazione avviene con le stesse forme previste nelle condizioni generali di fornitura.

art. 10 Legge applicabile, lingua applicabile, Controversie e foro esclusivo

10.01 Per quanto attiene alla legge applicabile, alla lingua applicabile ed al foro applicabile si fa riferimento alle condizioni generali di fornitura.

SEZIONE II
MISURE DI SICUREZZA

art. 11 Misure di sicurezza adeguate del responsabile del trattamento

11.01 CORETECH, quale responsabile del trattamento, si impegna nell'ambito dei trattamenti previsti dal presente accordo, relativi alla fornitura dei servizi informatici sopra descritti, ad adottare le misure tecniche ed organizzative adeguate, secondo standard tecnici di mercato, al fine di consentire la tutela della liceità dei trattamenti dei dati personali, la loro riservatezza, integrità, disponibilità e la resilienza dei servizi forniti.

11.02 CORETECH dichiara di aver predisposto un piano di gestione della sicurezza delle informazioni e di conformità alla privacy, in cui sono sintetizzate le misure di protezione per realizzare una gestione dei propri servizi nel rispetto del comma precedente.

11.03 Una sintesi delle misure di protezione adottate sono contenute nella scheda tecnica A) allegata al presente accordo.

11.04 CORETECH potrà aggiornare le misure di protezione per mantenere o aumentare i livelli di sicurezza dei servizi e all'uopo troverà applicazione il contratto di servizi circa le modalità operative.

11.05 In ogni caso resta inteso che CORETCH, al fine di tutelare i dati personali ad essa affidati con il presente accordo, potrà adottare tutte le misure, anche straordinarie, previste dal contratto di fornitura, compresa la sospensione dei servizi.

11.06 Qualora il CLIENTE richieda di adottare misure tecniche ed organizzative ulteriori, CORETECH si riserva di verificare la fattibilità della richiesta e di concordare se del caso, le modalità ed i costi relativi.

11.07 Il CLIENTE prima di accettare il presente accordo, ha verificato le misure di sicurezza sopra indicate, riscontrandole idonee all'ambito del trattamento dati da esso effettuato.

art. 12 Verifiche e controlli

12.01 Il responsabile del trattamento sottopone ad audit periodici il proprio sistema di gestione delle informazioni e piano di conformità alla privacy, di cui redige un rapporto scritto. Qualora ritenuto opportuno, lo stesso effettuerà anche audit di terze parti secondo standard internazionali e/best practice.

12.02 Al fine di dimostrare gli adempimenti al presente accordo, il responsabile del trattamento potrà anche esibire al CLIENTE, presso la propria sede, la documentazione di cui al comma precedente, senza estrazione di copia e verrà verbalizzata la verifica e gli esiti.

12.03 Resta salva la facoltà del CLIENTE di poter effettuare, a proprie spese, degli audit di terze parti al fine di verificare gli adempimenti al presente accordo, tramite proprio personale specializzato o professionisti di provata esperienza, in ogni caso vincolati per iscritto ad obblighi di riservatezza. CORETECH potrà opporsi alla nomina di professionisti che siano in conflitto di interesse, non sufficientemente qualificati o non indipendenti e in questo caso il CLIENTE dovrà proporre un diverso nominativo o svolgere direttamente l'audit. La relazione dell'audit, sarà messa a disposizione del responsabile del procedimento gratuitamente.

12.04 Le modalità di svolgimento dell'audit di cui al punto precedente saranno concordate dalle parti, e CORETECH comunicherà il costo orario del proprio personale incaricato di assistervi, comunque non inferiore alla tariffa oraria per l'assistenza tecnica.

12.05 Le attività di verifica che interessino eventuali sub-responsabili nominati da CORETECH saranno svolte secondo le modalità concordate con questi ultimi, nel rispetto delle loro politiche di conformità alla privacy.

art. 13 Misure di sicurezza del CLIENTE

13.01 Il CLIENTE è consapevole che la fruizione e la sicurezza dei servizi acquistati da CORETECH richiede una idonea configurazione dei servizi, che viene decisa in autonomia dal CLIENTE secondo le condizioni generali di fornitura.

13.02 Il CLIENTE si impegna a configurare, per quanto di sua competenza, i servizi suddetti in modo da garantire un adeguato livello di protezione in relazione al proprio ambito di trattamento dei dati personali nel rispetto della normativa sulla privacy.

13.03 In ogni caso, il CLIENTE terrà prontamente informata CORETECH nel caso sospetti o constati violazioni di sicurezza dei servizi acquistati, fornendo idonea documentazione al riguardo.

art. 14 Prodotti di terze parti

14.01 Resta inteso tra le parti che nel caso vengano utilizzati dal CLIENTE sui servizi di CORETECH componenti o servizi di terze parti, quest'ultima non sarà responsabile della loro gestione anche in relazione alle misure di protezione per la conformità alla normativa privacy.

art. 15 Violazioni di dati personali (Data Breach)

15.01 Nel caso CORETECH venga a conoscenza di un evento che stia dando luogo o possa aver dato luogo ad una violazione dei dati personali di cui al presente accordo, informerà il CLIENTE il prima possibile, con le modalità previste nel contratto di assistenza, trasferendo le informazioni a sua disposizione.
In ogni caso CORETECH invierà al CLIENTE, senza ritardo e per quanto ragionevolmente possibile, una relazione scritta che descriva i possibili danni cagionati e le cause se conosciute, le misure di protezione adottate per evitare o mitigare i potenziali rischi e suggerendo al CLIENTE le misure opportune a tutela dei dati personali trattati. Quest'ultimo verrà comunque tenuto sempre costantemente aggiornato.

15.02 Resta inteso che la comunicazione di cui sopra non costituisce riconoscimento di un inadempimento o responsabilità in capo al responsabile del trattamento, in relazione alla violazione ivi riportata.

15.03 Le parti concordano che nel rispetto dell'art. 33 e 34 del GDPR, spetti al CLIENTE effettuare le comunicazioni ivi previste all'Autorità Garante sotto la sua esclusiva responsabilità.

art. 16 Assistenza al CLIENTE per la conformità alla normativa privacy

16.01 Il responsabile del trattamento si impegna ad assistere il CLIENTE nel garantire il rispetto degli obblighi previsti dalla normativa privacy per quanto attiene ai servizi forniti, in particolare anche per quanto riguarda gli adempimenti relativi ai principi di minimizzazione del trattamento dei dati personali (*privacy by design* & *privacy by default*), nonché per quanto attiene alla valutazione di impatto protezione dati (DPIA) e consultazione preventiva.

16.02 In relazione al punto precedente, il responsabile del trattamento sarà tenuto solo alla fornitura delle informazioni relative ai servizi forniti che possano essere utili al CLIENTE e che rappresentino le modalità standard con cui essi vengono configurati e prestati.

16.03 Nel caso il CLIENTE richieda un'assistenza personalizzata in relazione al tipo di servizio che intende configurare nell'ambito della propria autonomia, CORETECH avrà diritto ad un corrispettivo che sarà concordato con il CLIENTE insieme con le relative modalità di svolgimento dell'assistenza richiesta.

SEZIONE III
TUTELA DEI DIRITTI DEGLI INTERESSATI

art. 17 Richieste di interessati al responsabile del trattamento e obblighi delle parti

17.01 Nel caso in cui il responsabile del trattamento riceva richieste per l'esercizio di diritti da parte di interessati in relazione a dati personali che tratta per conto del CLIENTE in base al presente accordo, sarà tenuto ad inviarle senza ritardo al CLIENTE, il quale si occuperà di gestire le suddette richieste, direttamente o anche tramite il titolare del trattamento se diverso dal CLIENTE stesso.

17.02 Il responsabile del trattamento assisterà il CLIENTE fornendogli tutte le informazioni in relazione ai servizi gestiti da CORETECH sulla base di quanto previsto dal presente accordo ed inviterà l'interessato a rivolgersi al CLIENTE al fine di esercitare i propri diritti, evidenziando la propria posizione di responsabile del trattamento.

17.03 Il CLIENTE si assume quindi ogni adempimento circa la gestione dei diritti degli interessati, salvo quanto indicato nei due commi precedenti relativamente al responsabile del trattamento.

art. 18 Richieste di interessati rivolte al CLIENTE per dati personali trattati per suo conto dal responsabile del trattamento

18.01 Nel caso in cui il CLIENTE debba soddisfare richieste relative ad interessati per l'esercizio dei loro diritti in relazione a dati personali oggetto del presente accordo, il responsabile del trattamento fornirà le informazioni richieste dal CLIENTE per quanto inerenti al presente accordo, in relazione ai servizi acquistati dal CLIENTE.

18.02 In ogni caso il CLIENTE tratterà direttamente la suddetta richiesta, limitandosi il responsabile del trattamento ad adempiere a quanto sopra.

art. 19 Portabilità dei dati personali

19.01 Nel caso in cui sia necessario da parte del CLIENTE soddisfare richieste di portabilità dei dati personali, il responsabile del trattamento fornirà, esclusivamente in relazione ai servizi acquistati dal CLIENTE, solo le informazioni utili per estrarli in formato conforme alla normativa sulla privacy e sempreché ciò sia ragionevolmente possibile.

19.02 Nel caso in cui il CLIENTE richieda invece l'assistenza tecnica necessaria per effettuare la suddetta estrazione, CORETECH ne valuterà la fattibilità tecnica e concorderà con il primo, se del caso, le modalità relative e i costi a carico del CLIENTE.

SEZIONE IV
DISPOSIZIONI FINALI

art. 20 Facoltà di modifica dell'accordo da parte del responsabile

20.01 CORETECH ha la facoltà di modificare le condizioni previste per il presente accordo nel rispetto della normativa sulla privacy, secondo quanto previsto dalle condizioni generali di fornitura, ferma restando la facoltà del CLIENTE di poter recedere.

art. 21 Obbligo di manleva a carico del CLIENTE

21.01 Per tutte le attività svolte in violazione della normativa sulla privacy, colposamente o dolosamente commesse dal CLIENTE utilizzando i servizi forniti dalla CORETECH, dalle quali possa derivare a carico di quest'ultima qualsivoglia pretesa stragiudiziale o giudiziale, anche correlata alla violazione delle presenti condizioni da parte del CLIENTE, questi si impegna ad assumersi ogni responsabilità ed a manlevarla e tenerla indenne il prima possibile, liberandola dalle suddette pretese.

21.02 Il CLIENTE dovrà sostenere direttamente ogni tipo di costo, risarcimento di danni ed oneri, incluse le eventuali spese professionali, che dovessero scaturire da tali pretese, oltre ad ogni ulteriore danno subito da CORETECH.

21.03 Resta salva la possibilità per il CLIENTE di provare la responsabilità di CORETECH per violazione del presente accordo.

21.04 Il CLIENTE informerà CORETECH, il prima possibile, di eventuali azioni che dovessero essere ad essa intentate.

art. 22 Prevalenza del presente accordo

22.01 Il presente accordo sostituisce qualsiasi altro accordo o istruzione antecedente relativa alla gestione dei dati personali in merito ai servizi forniti da CORETECH.

SEZIONE V
SCHEDA TECNICA ALLEGATA

MISURE DI PROTEZIONE ADOTTATE DAL RESPONSABILE DEL TRATTAMENTO

A) MISURE ORGANIZZATIVE	A-1) Adozione di una **politica sulla gestione della sicurezza delle informazioni** e **di una politica per la tutela dei dati personali** in conformità alla normativa privacy, basate sull'analisi del rischio, al fine di garantire la riservatezza, disponibilità ed integrità dei dati personali a tutela dei diritti e libertà degli interessati; A-2) **Procedure di accesso alle strutture fisiche,** debitamente protette, solo a soggetti autorizzati previo idoneo riconoscimento; A-3) **Policy e Disciplinari utenti**: Vengono applicate dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai servizi informatici deve conformarsi a garanzia della sicurezza dei sistemi;

A-4) **Autorizzazione accessi logici** – Tutti i sistemi informatici sono accessibili solo con profili di accesso per quanto necessario alla mansione svolta. I profili di autorizzazione sono individuati e configurati preventivamente all'accesso;

A-5) **Presente una procedura di gestione degli incidenti** collegata a strumenti tecnici di monitoraggio dei sistemi cui è proposto personale specializzato, con individuazione, in caso di incidente, degli interventi da predisporre secondo un ordine logicamente determinato, con lo scopo di garantire il ripristino dei servizi nel più breve tempo possibile, nonché verificarne le conseguenze, redigere un report, dal cui esito dipendono ulteriori misure di protezione, ferma in ogni caso la verifica dell'adeguatezza dei sistemi di protezione predisposti;

A-6) **Procedura di gestione dell'assistenza** – Gli interventi di assistenza vengono gestiti mediante una procedura che verifichi l'autenticità della richiesta ed eroghi il supporto contenendo al minimo il trattamento dati personali, tramite personale debitamente formato e strumenti tecnici rispetosi degli standard di sicurezza. Anche tramite un **servizio di ticket system** messo a disposizione del CLIENTE, sarà sempre possibile sapere il dettaglio dell'intervento, durata, data e l'operatore (tramite un codice univoco a lui assegnato), nonché verificare, da parte del responsabile del trattamento, l'autenticità della richiesta di supporto;

A-7) **In ogni caso i livelli di accesso ai sistemi del CLIENTE per fornire assistenza tecnica** saranno assegnati solo ad alcuni dipendenti specificamente autorizzati con credenziali di autenticazione conformi a standard internazionali;

A-8) **Impegno alla riservatezza** per iscritto di tutti i dipendenti prima di accedere ai sistemi;

A-9) Ogni **dipendente** può trattare solo le informazioni per i quali è stato **autorizzato** in relazione alle mansioni svolte nonché debitamente **formato**, mediante aggiornamenti periodici, per trattare i dati con la massima riservatezza e sicurezza, nel rispetto della normativa privacy;

A-10) **Regolamento interno per i dipendenti,** circa l'utilizzo degli strumenti informatici e sui potenziali controlli del datore di lavoro;

A-11) **Procedure di protezione contro attacchi tramite social engineering** con collegata specifica formazione del personale;

A-12) **Procedure per la scelta dei fornitori adeguati** incentrate sulla verifica di qualità, sicurezza e conformità alla normativa vigente dei beni o servizi offerti;

A-13) **Procedura di verifica della necessità di una DPIA, Valutazione d'impatto sulla protezione dei dati** in relazione ai sistemi informatici utilizzati in base alla normativa privacy;

	A-14) **Data Breach** – Esiste una procedura per la gestione degli incidenti che possa incidere sui dati personali, basata sulla distribuzione dei ruoli secondo competenza, verifica del potenziale pregiudizio (presunto o accertato), gestione delle contromisure nonché le modalità di condivisione con il CLIENTE delle informazioni relative alle violazioni di dati personali e per l'adozione degli adempimenti connessi previsti dalla normativa privacy; A-15) **Procedure per lo smaltimento** della documentazione analogica e dei sistemi informatici potenzialmente contenenti informazioni, tramite idonei strumenti (quali distruggi documenti e ditte certificate nello smaltimento); A-16) **Aggiornamento delle misure organizzative** che saranno verificate ogni sei mesi;
B) MISURE TECNICHE	B-1) **Credenziali di autenticazione** – L'accesso ai sistemi si basa esclusivamente su credenziali di autenticazione univoche, basate su un PIN o chiave di accesso riservate e con misure di sicurezza conformi a standard internazionali; B-2) **Gestione password di accesso** secondo *best practise*, basate sulla lunghezza, complessità, scadenza, robustezza affidate a soggetti debitamente istruiti circa il suo utilizzo e conservazione; B-3) **Amministratori di Sistema** – Per gli utenti con ruolo di Amministratori di Sistema, le cui mansioni sono attribuite con atti di nomina specifici ed in forma scritta, è implementato un sistema di log management non alterabile debitamente configurato per tracciare le attività svolte e consentire il monitoraggio successivo per la verifica della regolarità delle operazioni. E' attiva poi una procedura per la verifica dell'operato degli amministratori di sistema nell'ambito del piano di sicurezza delle informazioni elaborato internamente e per la conformità rispetto alla normativa sulla privacy ed anche al fine del miglioramento delle misure di protezione; B-4) **Utilizzo di sistemi di cifratura** basati su algoritmi e protocolli informatici conformi a standard internazionali; B-5) **IDS/IPS Intrusion Detection System e Intrusion Prevention System** quali sistemi di rilevamento delle intrusioni, per individuare in anticipo attacchi informatici; B-6) **Adozione di sistemi Firewall** quali componenti di difesa perimetrale delle reti informatiche ed a tutela delle linee di comunicazione; B-7) **Antivirus e Malware** aggiornati con cadenza periodica contro il rischio di intrusione e dell'azione illecita di programmi;

	B-8) **Sistemi di logging** al fine del monitoraggio dei sistemi, conservazione degli eventi accaduti ed identificazione degli accessi; B-9) **Sistemi di backup & restore**, con relativa procedura di gestione; B-10) **Business continuity** per la resilienza dei sistemi in caso di incidente; B-11) **Vulnerability Assessment & Penetration Test** – Vengono eseguite periodicamente attività di analisi delle vulnerabilità dei sistemi sia in relazione agli ambiti infrastrutturali sia a quelli applicativi, nonché eseguiti Penetration Test con cadenza periodica, ipotizzando diversi scenari di attacco, con l'obiettivo di verificare il livello di sicurezza di applicazioni/sistemi/reti e quindi sulla base dei relativi report, migliorare le misure di sicurezza; B-12) Scelta **DATA CENTER** con standard TIER 4; B-13) **Aggiornamento constante dei sistemi informatici, delle misure tecniche**, al variare della tecnologia e con costante verifica secondo tempistiche prestabilite nonché **verifica costante, presso fonti affidabili, dei problemi di sicurezza dei prodotti e servizi informatici in uso** per l'update relativo.