



Cod. NF4 – P2
Cod. Cons/rg

Protocollo Generale (Uscita)
cnappcrm – aoo_generale

Prot.: 0000643

Data: 23/05/2024

Circolare n. 73

Ai Consigli degli Ordini degli Architetti,
Pianificatori, Paesaggisti e Conservatori
LORO SEDI

Oggetto: Impiego delle GCFP-API servizi di integrazione

Gentilissimi,

a seguito della richiesta di alcuni Ordini territoriali, di poter utilizzare l'applicativo che consente l'interfaccia tra la piattaforma per la gestione di corsi ed eventi formativi, in uso da parte degli Ordini e la piattaforma di Gestione dei Crediti Formativi Professionali gestita dal CNAPPC, questo Consiglio Nazionale, nella seduta dell'8 maggio u.s., ha espresso esito favorevole, al fine di agevolare l'attività suddetta.

Pertanto, gli Ordini interessati potranno comunicare la propria adesione, rinviando i seguenti allegati, debitamente compilati e sottoscritti, all'indirizzo direzione@cnappc.it

1. *Informazioni tecniche per l'accesso alle API di integrazione alla piattaforma GCFP*
2. *Accordo sulla protezione dei dati personali*
3. *Procura per la selezione dei responsabili del trattamento*
4. *Scheda relativa all'organizzazione del Responsabile del Trattamento*

Qualora l'Ordine o suo fornitore, desiderassero usufruire della consulenza della società Didanet, relativamente ad esigenze specifiche legate al progetto, si comunica che il CNAPPC ha chiesto ed ottenuto in tal senso, un'offerta economica convenzionata (all.5) che potrà essere sottoscritta direttamente con il fornitore.

Eventuali chiarimenti possono essere richiesti all'indirizzo: esteri@cnappc.it

Cordiali saluti.

*Il Responsabile del Dipartimento
Formazione*

(Flavio Mangione)

Il Consigliere Segretario

(Tiziana Campus)

Il Presidente

(Massimo Crusi)

- ALL:**
1. *Informazioni tecniche per l'accesso alle API di integrazione alla piattaforma GCFP*
 2. *Accordo sulla protezione dei dati personali*
 3. *Procura per la selezione dei responsabili del trattamento*
 4. *Scheda relativa all'organizzazione del Responsabile del Trattamento*
 5. *Contratto attività di assistenza Didanet*

Accordo sulla protezione dei dati personali ai sensi dell'art. 28 del Regolamento EU 679/2016

Data Processing Agreement (DPA)

Tra il Titolare del trattamento e il Responsabile del trattamento

l'Ordine degli Architetti Paesaggisti Pianificatori e Conservatori della Provincia di _____, con sede in _____, n. __ – CAP _____ Provincia _____ in persona del Presidente del Consiglio dell'Ordine e legale rappresentante, sig. _____ (qui di seguito, anche "Titolare del trattamento" o "Titolare" o "Ordine")

da una parte, e

[...] con sede legale in [...] e rappresentato da [...] (qui di seguito, anche "Responsabile del trattamento" o "Responsabile")

PREMESSO CHE

A. tra le parti è in essere un contratto in forza del quale [...] svolge in favore dell'Ordine i seguenti servizi:

(qui di seguito "Servizi")

B. per poter espletare i Servizi _____ si trova a dover trattare per conto dell'Ordine i dati personali di soggetti estranei al presente contratto (qui di seguito "Interessati") rispetto ai quali quest'ultimo è Titolare del trattamento (o Responsabile del trattamento per conto di altro titolare);

C. si richiamano tutte le definizioni contenute nell'art. 4 del Regolamento (Ue) 2016/679 (qui di seguito anche "GDPR") sulla protezione dei dati e, segnatamente, quelle di:

- "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;
- "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;

- “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;
- “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;

D. in forza di tali previsioni, _____ riveste la posizione di Responsabile del trattamento in relazione ai dati personali di terzi che l’Ordine comunicherà, trasferirà o, comunque, metterà a sua disposizione ai fini dell’espletamento dei Servizi (di seguito “**Dati personali**”);

E. sulla base delle referenze e competenze vantate da _____ in termini di proprietà, uomini, attrezzature ed esperienza nel campo del trattamento dei dati in generale, l’Ordine ha condotto una positiva valutazione della sua idoneità a soddisfare, anche sotto il profilo della sicurezza del trattamento, i necessari standard di esperienza, capacità ed affidabilità previsti dalla normativa applicabile in materia di protezione dei dati personali onde assicurare le richieste garanzie di legge;

F. il Responsabile del trattamento effettua il trattamento secondo le istruzioni impartite dal Titolare del trattamento, assicurando l’adozione di misure tecniche e organizzative adeguate al fine di assicurare che il trattamento soddisfi i requisiti delle normative vigenti in materia di trattamento dei dati personali e garantisca la tutela dei diritti dell’interessato. (art. 28, par. 1 GDPR);

G. il Responsabile del trattamento è vincolato al Titolare del trattamento mediante contratto o altro atto giuridico, con il quale è disciplinata la materia e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento e gli obblighi e i diritti del responsabile del trattamento (art. 28, par. 3 GDPR);

tanto premesso, si conviene e stipula quanto di seguito riportato.

Premesse

Le premesse costituiscono parte integrante e sostanziale del presente contratto.

Designazione del Responsabile del trattamento

Con il presente atto, il Titolare del trattamento, designa _____ - che accetta - quale Responsabile del trattamento, nei limiti di quanto necessario per l’espletamento dei Servizi.

Oggetto del presente contratto

Oggetto del presente contratto è la definizione delle modalità secondo le quali il Responsabile del trattamento si impegna ad effettuare, per conto del Titolare, le operazioni di trattamento dei Dati personali.

Nel quadro delle loro relazioni contrattuali, le parti si impegnano a rispettare la regolamentazione in vigore applicabile al trattamento dei Dati personali e, in particolare, il GDPR.

Descrizione delle prestazioni del Responsabile del trattamento

Il Responsabile del trattamento è autorizzato a trattare per conto del Titolare del trattamento i Dati personali necessari per fornire i Servizi, con o senza l’ausilio di strumenti elettronici o comunque automatizzati, nel pieno rispetto delle norme previste dal GDPR, nonché di quanto disposto dalle istruzioni operative impartite dal Titolare del trattamento.

I dati si riferiscono alle seguenti categorie di Interessati:

-
-

Tale autorizzazione è limitata a quanto indispensabile al fine dell'espletamento dei Servizi, nonché ai soli Dati personali trasferiti dal Titolare del trattamento appartenenti alle seguenti categorie:

-
- ...
- ...
- ...

Qualora la documentazione trasferita al Responsabile del trattamento dovesse contenere informazioni eccedenti e/o non pertinenti con le anzidette finalità, soprattutto se qualificabili come “*dati particolari*” ai sensi dell’art. 9 GDPR, il Responsabile del trattamento si impegna a non utilizzarli in alcun modo e, qualora sia possibile separarli, a cancellarli in condizioni di sicurezza.

Durata del contratto

Gli accordi di cui al presente contratto si intendono validi per tutta la durata del rapporto sottostante tra le parti e, quindi, fino a quando il Responsabile del trattamento continuerà a espletare i Servizi in favore del Titolare del Trattamento.

Alla conclusione del rapporto il Responsabile del trattamento s’impegna a restituire tutti i Dati personali e cancellare le copie esistenti nell’osservanza dei principi di sicurezza e riservatezza, salvo che la conservazione dei dati sia prevista dal diritto dell’UE o da quello interno.

Sub-Responsabili

Il Responsabile del trattamento può a sua volta ricorrere ad un altro Responsabile del trattamento (di seguito, “**Sub-Responsabile**”) per gestire, in tutto o in parte, specifiche attività di trattamento rientranti tra quelle regolate dal presente accordo.

In questo caso, ne informa preventivamente e per iscritto il Titolare del trattamento, indicando chiaramente l’identità e i recapiti del Sub-Responsabile e le attività di trattamento che intende affidare a quest’ultimo, nonché le categorie di Dati personali e di Interessati coinvolte. Entro il termine di 15 giorni dal ricevimento di tale comunicazione, il Titolare del trattamento può opporsi.

Lo stesso procedimento si applica alla sostituzione dei Sub-Responsabili.

Spetta al Responsabile del trattamento assicurare che i Sub-Responsabili possano garantire il rispetto degli obblighi derivanti dal presente contratto per conto e secondo le istruzioni del Titolare del trattamento, anche stipulando con essi ulteriori contratti e/o altri atti giuridici aventi il medesimo contenuto.

Il Responsabile del trattamento risponde nei confronti del Titolare del trattamento degli eventuali inadempimenti imputabili ai Sub-Responsabili.

In caso di trasferimento dei Dati personali a fornitori di servizi ubicati al di fuori dell’Unione Europea, oppure verso sistemi tecnici gestiti in cloud e localizzati al di fuori dell’area dell’Unione Europea, il Responsabile del trattamento dovrà adottare tutte le cautele necessarie al fine di garantire la più totale protezione dei Dati personali, basando il trasferimento: a) su decisioni di adeguatezza dei paesi terzi destinatari espressi dalla Commissione Europea; b) su garanzie adeguate espresse dal soggetto terzo destinatario.

Obblighi del Responsabile del trattamento

Il Responsabile del trattamento si impegna a:

1. trattare i Dati personali nei limiti di quanto strettamente necessario per l’espletamento dei

Servizi;

2. porre in atto nell'organizzazione della propria attività le misure di sicurezza necessarie in base alla normativa in vigore per il trattamento dei dati personali ed a svolgere le proprie prestazioni nel rispetto delle istruzioni contenute nel presente contratto o ricevute dal Titolare del trattamento, mettendo a disposizione di quest'ultimo la documentazione necessaria a comprovare il rispetto di tale obbligo;
3. informare immediatamente il Titolare del trattamento se ritiene che una sua istruzione costituisca una violazione del GDPR o di tutte le altre disposizioni delle leggi dell'UE o delle leggi degli stati membri relative alla protezione dei dati;
4. trattare i Dati personali in modo lecito e secondo correttezza e trasparenza, nel rispetto dei principi di minimizzazione, esattezza, limitazione e riservatezza, come definiti dall'art. 5 GDPR;
5. adottare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato ai rischi di perdita, danneggiamenti ed accessi non autorizzati, ai sensi degli artt. 32 GDPR e verificarne la costante adeguatezza; segnalare tempestivamente e rimuovere qualsiasi eventuale carenza sulle misure di sicurezza adottate;
6. tenere conto, nell'utilizzare materiali, prodotti, applicazioni o servizi ai fini delle proprie attività, fin da quando questi vengono progettati o messi in uso, dei principi di "privacy by design" e "privacy by default" come definiti dall'art. 25 GDPR.
7. designare le persone autorizzate al trattamento, assicurando che esse siano adeguatamente formate in materia di protezione dei dati personali e si impegnino a rispettare la riservatezza dei Dati personali o siano sottoposti ad un obbligo legale appropriato di segretezza;
8. rispettare e far rispettare alle persone autorizzate al trattamento, nonché agli altri soggetti che per qualsivoglia motivo entreranno in contatto con i Dati personali, tutte le misure di sicurezza già attuate o che verranno in futuro predisposte;
9. archiviare, custodire e conservare i Dati personali – compresi i documenti elettronici – per tutta la durata del presente contratto, fatto salvo il rispetto di eventuali termini di legge stabiliti per alcune categorie di dati e/o documenti;
10. verificare con cadenza almeno annuale che i profili di accesso assegnati alle persone autorizzate al trattamento siano adeguati e non eccedenti rispetto alle esigenze della mansione o della unità organizzativa cui gli stessi sono stati assegnati;
11. eventualmente, assistere il Titolare del trattamento nel processo di valutazione d'impatto sulla protezione dei dati (DPIA – Data Protection Impact Assessment) di cui all'art. 35 GDPR, nonché nella consultazione preventiva con l'Autorità di controllo ai sensi dell'art. 36 GDPR, qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare per attenuare il rischio;
12. comunicare al Titolare del trattamento senza ritardo, comunque entro 24 ore, eventuali reclami provenienti dagli Interessati e contestazioni, ispezioni o richieste ricevute da parte dell'Autorità di controllo e/o delle Autorità Giudiziarie; informare prontamente il Titolare del trattamento di ogni altra notizia rilevante, comprese nuove attività di trattamento che dovesse mettere in atto;
13. tenere costantemente aggiornato presso di sé, ed a disposizione in ogni momento del Titolare del trattamento, un registro di tutte le categorie di attività relative al trattamento svolte per conto del Titolare, ai sensi dell'art. 30 GDPR, in forma scritta, anche in formato elettronico.
14. predisporre ed eseguire una periodica attività di verifica interna sull'operato dei propri Sub-responsabili ed autorizzati al trattamento;
15. collaborare con il Titolare del trattamento per revisione delle attività di trattamento svolte,

acconsentendo, a tal fine, anche all'esecuzione di appositi controlli (audit) presso le sue strutture e i suoi dipendenti/collaboratori da parte del Titolare o di un soggetto dallo stesso incaricato;

Esercizio dei diritti degli Interessati

Il Responsabile del trattamento deve collaborare con il Titolare del trattamento, per quanto di sua competenza, al fine di soddisfare l'obbligo di quest'ultimo di dare seguito alle richieste per l'esercizio dei diritti degli Interessati e fornire tutto il supporto necessario al fine di consentire una risposta nei termini indicati dal GDPR.

Qualora l'Interessato rivolga la propria istanza per l'esercizio di uno dei propri diritti direttamente al Responsabile del trattamento, quest'ultimo dovrà inoltrarla al Titolare del trattamento senza ritardo e comunque entro 24 ore dal ricevimento.

Notifica della violazione di Dati personali (data breach)

In caso di violazione dei Dati personali, il Responsabile del trattamento si impegna a comunicarla al Titolare del trattamento senza ingiustificato ritardo e non al più tardi di 12 ore dal momento in cui ha conoscenza della violazione.

Tale comunicazione è accompagnata da ogni documentazione utile per permettere al Titolare del trattamento, se necessario, di notificare questa violazione all'autorità di controllo competente e deve, almeno:

- a) descrivere la natura della violazione indicando, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei Dati personali in questione;
- b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati (DPO), se nominato, o di altro punto di contatto presso cui ottenere più informazioni;
- c) descrivere le probabili conseguenze della violazione dei Dati personali;
- d) 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.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le stesse possono essere comunicate in fasi successive senza ulteriore ingiustificato ritardo.

Obblighi del Titolare del trattamento

Il Titolare del trattamento s'impegna a fornire al Responsabile del trattamento i Dati personali e a documentare per iscritto tutte le istruzioni riguardanti il loro trattamento da parte del Responsabile del trattamento che non inserite nel presente contratto.

Manleva contrattuale

Il Responsabile del trattamento si obbliga a rimborsare e tenere indenne il Titolare del trattamento per ogni somma da quest'ultimo eventualmente versata e/o pagata come sanzione e/o come risarcimento di danni a Interessati e/o terzi a causa del trattamento dei Dati personali non conforme alle previsioni del GDPR per motivi imputabili all'inosservanza dei presenti accordi da parte del Responsabile del trattamento.

Clausola risolutiva espressa

In caso di perdita da parte del Responsabile del trattamento dei requisiti di cui all'art. 28 GDPR e/o di suo inadempimento alle disposizioni di legge in materia di protezione dei dati personali o dei presenti accordi, il Titolare del trattamento potrà risolvere il contratto, ai sensi dell'art. 1456 cod.civ., con conseguente revoca automatica della designazione in oggetto. Ciò comporterà anche la risoluzione del contratto o del rapporto intercorrente tra le parti per l'espletamento dei

Servizi, in tutti i casi in cui essi non possano essere forniti senza il trattamento dei Dati personali.

Estensione

I presenti accordi si applicano anche al caso in cui la L'Ordine agisca in qualità di Responsabile del trattamento dei dati per conto di altro titolare terzo. In tal caso, la _____ ricoprirà il ruolo di Sub – Responsabile del trattamento.

Luogo e data _____

II TITOLARE DEL TRATTAMENTO

IL RESPONSABILE DEL TRATTAMENTO

Per accettazione espressa degli accordi contenuti nei seguenti articoli:

- Sub-Responsabili
- Obblighi del Responsabile del trattamento
- Manleva contrattuale
- Clausola risolutiva espressa

Luogo e data _____

II TITOLARE DEL TRATTAMENTO

IL RESPONSABILE DEL TRATTAMENTO

SCHEDA RIEPILOGATIVA DEI TRATTAMENTI DEL RESPONSABILE ESTERNO

A. DATI ACCESSIBILI *(barrare solo i dati accessibili):*

Personalì (art. 4 p. 1 GDPR)

- Dati Anagrafici (nome, cognome, data e luogo di nascita)
- Codice fiscale, partita IVA ed altri numeri di identificazione personale
- Luogo e indirizzo di residenza
- Dati relativi a sanzioni disciplinari
- Dati di LOG e/o indirizzi IP
- Dati relativi all'attività professionale e all'iscrizione in albi
- Nominativo, indirizzo o altri elementi di identificazione personale
- Dati relativi alla famiglia e a situazioni personali
- Informazioni relative all'attività lavorativa svolta (presenze, permessi, carichi di lavoro dei propri dipendenti, ecc.)
- Attività economiche, commerciali, finanziarie e assicurative
- Dati Bancari e/o assicurativi
- Istruzione e cultura
- Indirizzo di posta elettronica contenenti generalità di persone fisiche e PEC
- Fotografie e riprese filmate
- Dati di LOG e/o indirizzi IP
- Dati relativi alla formazione professionale degli iscritti
- Altro (specificare) _____

Categorie particolari di dati personali (art. 9 GDPR)

- l'origine razziale o etnica
- le opinioni politiche
- le convinzioni filosofiche o religiose
- l'appartenenza sindacale
- dati genetici
- dati biometrici intesi ad identificare in modo univoco una persona fisica
- dati relativi alla salute o alla vita sessuale o all'orientamento sessuale

Relativi a condanne penali o reati (art. 10 GDPR)

- relativi a condanne penali e ai reati
- relativi a connesse misure di sicurezza (sulla base di quanto previsto all'art. 6 §1 GDPR)

B. CATEGORIE DI TRATTAMENTO

Le attività di trattamento (art. 4 n.2) effettuabili consistono in *(barrare solo i trattamenti consentiti):*

- | | |
|---|---|
| <input type="checkbox"/> raccolta | <input type="checkbox"/> consultazione |
| <input type="checkbox"/> registrazione | <input type="checkbox"/> utilizzo |
| <input type="checkbox"/> organizzazione | <input type="checkbox"/> comunicazione mediante trasmissione |
| <input type="checkbox"/> strutturazione | <input type="checkbox"/> diffusione o qualsiasi altra forma di messa a disposizione |
| <input type="checkbox"/> conservazione | <input type="checkbox"/> raffronto |
| <input type="checkbox"/> adattamento | <input type="checkbox"/> interconnessione |
| <input type="checkbox"/> modificazione | <input type="checkbox"/> limitazione |
| <input type="checkbox"/> selezione | <input type="checkbox"/> cancellazione |
| <input type="checkbox"/> estrazione | <input type="checkbox"/> distruzione |

C. MODALITA' DI TRATTAMENTO (barrare solo le modalità utilizzate e specificare le informazioni richieste):

- Back up sui server di rete
- Back up in cloud fornito da _____
- Software gestionale fornito da _____
- Software di posta elettronica fornito da _____
- Sito internet fornito da _____
- Luogo di conservazione
- Modalità di eliminazione (al termine del trattamento)
- Interconnessione LAN (Local Area Network per la comunicazione interna)
- Interconnessione Internal VPN per interconnessione tra sedi
- Supporti rimovibili di memorizzazione (CD Memory Card Hard disk esterni Chiavette USB)

D. FINALITA' DI TRATTAMENTO

- Gestione/Amministrazione del personale
- Recruitment
- Gestione banche/assicurazione
- Compliance e Sistemi di gestione (es. D. 81/08 - D. Lgs 231/01 - Privacy - Antiriciclaggio)
- Controllo accessi/Sicurezza fisica
- Gestione del contenzioso/Gestione crediti
- Partecipazione a gare / Progetti finanziati
- Amministrazione/Contabilità/ Finanza
- Assistenza clienti
- Pubbliche relazioni
- Marketing diretto/Informazioni commerciali
- Digital Marketing
- Ricerche di mercato/Analisi generale della clientela
- Profilazione
- Ricerca storica o statistica
- Medicina del lavoro
- Prevenzione frodi / Sicurezza informatica

PROCEDURA PER LA SELEZIONE DEI RESPONSABILI DEL TRATTAMENTO

Regolamento UE 2016/679 - GDPR

Codice della Privacy D.Lgs. 196/2003 e succ. modd.

Prima adozione____

Revisione del _____ autore della revisione_____

Revisione del _____ autore della revisione_____

Revisione del _____ autore della revisione_____

Sommario

DEFINIZIONI.....	2
SCOPO/AMBITO DI APPLICAZIONE	2
INDIVIDUAZIONE DEL FORNITORE E STIPULA DELL'ATTO DI IDENTIFICAZIONE.....	3
CLAUSOLA DI PROTEZIONE DEI DATI PERSONALI.....	Errore. Il segnalibro non è definito.
ADEMPIMENTI SUCCESSIVI ALLA SOTTOSCRIZIONE DELL'ATTO DI NOMINA.....	4
INTEGRAZIONI E MODIFICHE	Errore. Il segnalibro non è definito.
Allegato 1	Errore. Il segnalibro non è definito.
Allegato 2	Errore. Il segnalibro non è definito.

RIFERIMENTI

- ☒ Regolamento (UE) 2016/679 “**GDPR**”;
- ☒ Sistema di gestione per la protezione dei dati personali (D’ora in avanti “**SGP**”);
- ☒ Registro dei trattamenti
- ☒ Registro dei Responsabili del trattamento.

DEFINIZIONI

- **l’Ordine:** l’Ordine degli Architetti P.P.C. di _____;
- **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;
- **Interessati:** le persone fisiche a cui i Dati personali si riferiscono;
- **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;
- **Titolare del trattamento o Titolare:** 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;
- **Responsabile del trattamento:** la persona fisica o giuridica, l’autorità pubblica, il servizio, altro organismo che tratta dati personali per conto del Titolare del trattamento;
- **Sub-responsabili del trattamento:** soggetti terzi, nominati dal Responsabile del trattamento mediante apposito atto di nomina che impone al Sub-responsabile gli stessi obblighi in materia di protezione dei dati contenuti nell’atto di nomina a Responsabile del trattamento.
- **Data Protection Officer o DPO:** figura professionale esperta nella protezione dei dati, il cui compito è valutare e organizzare la gestione del Trattamento dei dati personali, e dunque la loro protezione, all’interno dell’organizzazione del Titolare o del Responsabile del trattamento, affinché questi siano trattati in modo lecito e pertinente;
- **GDPR:** Regolamento Europeo 2016/679 sul Trattamento dei dati personali;

SCOPO/AMBITO DI APPLICAZIONE

Il Regolamento (UE) 2016/679 (GDPR) prevede che qualora un Trattamento venga effettuato per conto del Titolare da parte di un soggetto esterno, quest’ultimo deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell’interessato; a tal fine tale soggetto deve essere conseguentemente designato Responsabile del trattamento mediante contratto o altro atto giuridicamente valido.

Nel caso in cui l’Ordine agisca quale Responsabile del trattamento per conto di un Titolare-Committente, il fornitore esterno acquisisce la posizione di Sub-responsabile.

Lo scopo della presente procedura è quello di descrivere e regolamentare il processo di selezione e nomina a Responsabili del trattamento (o Sub-responsabili) dei fornitori, consulenti, appaltatori e subappaltatori che trattano dati per conto della dell’Ordine.

INDIVIDUAZIONE DEL FORNITORE E STIPULA DELL'ATTO DI IDENTIFICAZIONE

Il personale dell'Ordine verifica se il fornitore con cui deve essere sottoscritto un contratto tratta dati personali per conto dell'Ordine e se, conseguentemente, deve essere nominato Responsabile del trattamento (o Sub-responsabile) ai sensi dell'art. 28 del GDPR.

Ad esempio, un fornitore dovrà essere nominato Responsabile del trattamento qualora la prestazione contrattuale consista in (oppure comporti un) trattamento da parte del fornitore di dati personali di cui sia Titolare l'Ordine

In linea generale, l'Ordine è Titolare dei trattamenti per i quali abbia deciso (da solo o insieme con altri contitolari) le finalità e i mezzi. Nei casi in cui il trattamento avvenga in adempimento di obblighi di legge o per finalità di pubblico interesse, la titolarità può essere desunta dal fatto che vi sia una norma di legge, regolamento o atto amministrativo generale che individua l'Ordine come il soggetto deputato a porre in essere una certa attività di trattamento di dati personali.

I trattamenti di cui l'Ordine è Titolare sono indicati nel Registro dei trattamenti.

Per maggiori informazioni sui criteri utili per determinare quando ricorra lo status di Titolare e quando quella di Responsabile del trattamento, può essere utile consultare le Linee Guida n. 7/2020 dello European Data Protection Board al seguente link <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr-it>

In ogni caso di dubbio è necessario rivolgersi al DPO.

Nel caso in cui la l'Ordina agisca quale Responsabile del trattamento per conto di un altro Titolare-Committente, il personale dovrà prima di tutto accertarsi che gli accordi tra esso e il Titolare-Committente originario (con cui l'Ordine è stato nominato Responsabile del trattamento) non contenga un espresso divieto preventivo alla nomina di Sub-responsabili del trattamento.

L'atto di nomina dei Sub-responsabili deve contenere gli stessi obblighi in materia di protezione dei Dati personali contenuti nell'accordo intercorso tra Titolare-Committente e l'Ordine.

Una volta verificato che il fornitore con cui deve essere sottoscritto un contratto, tratterà dati personali per conto dell'Ordine, il personale coinvolto dovrà verificare che il fornitore si impegni, ai sensi dell'art. 28 GDPR, a prestare garanzie adeguate per il trattamento dei dati e che adotti a tal fine idonee misure tecniche e organizzative.

A tal fine, nella "**Scheda relativa all'organizzazione del Responsabile del trattamento**" allegata alla presente procedura (all. 4) sono contenute le misure tecniche ed organizzative che il fornitore mette in campo, al fine di essere in regola con la normativa di cui al GDPR e di garantire un'adeguata protezione dei dati personali trattati nel perimetro contrattuale.

La suddetta scheda deve essere consegnata al fornitore e restituita compilata in ogni sua parte (sono ammissibili delle risposte di "non applicabilità" di singole misure) e firmata.

Il Personale dell'Ordine, eventualmente con l'assistenza del DPO, dovrà poi esaminare le risposte ricevute, chiedere eventualmente dei chiarimenti o delle integrazioni e formulare una valutazione della complessiva adeguatezza delle misure tecniche e organizzative adottate del fornitore, rispetto al livello di rischio collegato al trattamento, come preventivamente misurato.

In caso di non conformità ritenute non bloccanti, il personale dell'Ordine potrà indicare al fornitore un termine di non più di sei mesi per l'adeguamento.

Contestualmente all'affidamento e alla sottoscrizione del contratto si dovrà provvedere anche alla

formalizzazione dell'atto di nomina del fornitore a Responsabile ex art. 28 GDPR.

A tal fine, all'atto della sottoscrizione del contratto, il personale dell'Ordine utilizza il "modello di accordo di nomina a responsabile del trattamento" messo a disposizione dall'Ordine stesso avendo cura di adeguarlo alle specifiche del singolo rapporto contrattuale.

Gli affidamenti che comportino il trasferimento di dati personali extra UE potranno essere ammessi solo previo controllo sulla sussistenza delle condizioni indicate nel GDPR.

ADEMPIMENTI SUCCESSIVI ALLA SOTTOSCRIZIONE DELL'ATTO DI NOMINA

A seguito della sottoscrizione dell'Accordo di nomina a Responsabile del trattamento, il personale dell'Ordine provvederà ad aggiornare il Registro dei trattamenti e il Registro dei Responsabili del trattamento.

Nel caso di rapporti continuativi nel tempo, il personale dell'Ordine programma le verifiche sul fornitore secondo le modalità e con le scadenze più opportune, eventualmente in collaborazione con il DPO o, in ogni caso, informando il DPO in merito agli esiti dei controlli.

Una volta cessato il rapporto contrattuale con il fornitore, il personale dell'Ordine provvede al tempestivo aggiornamento del Registro dei trattamenti e del registro dei Responsabili del trattamento.

Allegati:

- modello di accordo di nomina a responsabile del trattamento

All. 4) Scheda relativa all'organizzazione del Responsabile del trattamento.

Scheda relativa all'organizzazione del Responsabile del trattamento

Ordine degli Architetti Pianificatori Paesaggisti e Conservatori
della provincia di _____

Scheda relativa all'organizzazione del Responsabile del trattamento

Allegato all'accordo sul trattamento dei dati personali tra Titolare e responsabile del trattamento
Ai sensi dell'art. 28 del Reg. EU 2016/679

L'art. 28 del Regolamento Europeo 2016/679 (GDPR) prevede che il Titolare del trattamento, qualora affidi un trattamento a un Responsabile del trattamento, debba verificare che questi attui idonee misure tecnico-organizzative per garantire la conformità del trattamento alla normativa di riferimento e la tutela dei diritti degli interessati.

In particolare, anche il Responsabile del trattamento deve garantire l'adozione delle misure di sicurezza di cui all'art. 32 del GDPR.

Gli accordi tra Titolare e Responsabile devono essere recepiti in un accordo scritto in cui le parti disciplinano le finalità del trattamento (decise dal Titolare ed alle quali il Responsabile si deve attenere), la sua natura e trattamento, il tipo di dati personali e le categorie, di interessati, gli obblighi e i diritti delle parti.

Il presente documento costituisce allegato al suddetto accordo. Vi invitiamo a compilarlo al fine di valutare che le garanzie che la Vostra organizzazione presenta siano adeguate alla soddisfazione dei requisiti richiesti dal GDPR, nonché alla tutela dei diritti degli interessati coinvolti nel trattamento che effettua per conto del Titolare.

Le informazioni richieste si riferiscono al trattamento in perimetro contrattuale, ai sistemi informatici attraverso i quali esso viene effettuato e i relativi presidi di tipo fisico, tecnologico e organizzativo.

Responsabile del Trattamento	
Checklist completata da	
Data	

Sezione A – Dati e modalità del Trattamento

Domande		Risposte
1	Sono stati adottati presidi organizzativi o tecnologici per impedire che i dati personali siano trattati per finalità diverse da quelle indicate nell'accordo ex art. 28 GDPR e/o nel documento di nomina a responsabile del trattamento?	
2	Specificare i luoghi (indicando anche dove si trovano i server, se presenti) dove il Responsabile, gli autorizzati al trattamento e gli eventuali Sub-responsabili trattano i dati personali per conto del Titolare.	
3	Precisare se l'hosting e gli ulteriori trattamenti dei dati personali effettuati per conto del Titolare, sono limitati allo Spazio Economico Europeo (SEE).	
4	Nel caso in cui i dati personali siano trattati per conto del Titolare <u>al di fuori del SEE</u> , descrivere le misure di salvaguardia ai sensi degli artt. 46 e 47 GDPR per garantire che siano adeguatamente protetti al di fuori del SEE (per esempio: Clausole Contrattuali Standard Europee).	

Sezione B – Misure organizzative

Domande		Risposte
1	È stato delineato un sistema interno di deleghe di compiti e funzioni in materia di privacy?	<i>[In questo caso, si prega di descrivere a/ e misura/e adottate]</i>
2	Il personale che tratta dati in perimetro contrattuale è stato autorizzato al trattamento secondo profilazioni definite e nel rispetto del principio di minimizzazione del trattamento?	
3	Tutti gli autorizzati al trattamento hanno ricevuto le istruzioni per il trattamento dei dati personali nel quale sono coinvolti ?	
4	Tutte le persone autorizzate al trattamento partecipano a corsi di formazione incentrati sugli obblighi previsti dalle normative vigenti in tema di Protezione dei Dati e sulle procedure da applicare ai trattamenti in perimetro contrattuale?	
5	Avete adottato un registro delle attività di Trattamento ¹ (art 30 GDPR) in qualità di Responsabile? Se così fosse, questo registro è sempre aggiornato?	
6	È stato compilato un documento di valutazione dei rischi privacy in relazione ai trattamenti in perimetro contrattuale?	
7	Viene eseguita la valutazione di impatto privacy sul servizio rientrante nel perimetro contrattuale?	
8	È stato nominato il Data Protection Officer?	
9	Avete adottato misure organizzative interne volte a prevenire eventuali violazioni della riservatezza, integrità e disponibilità dei dati personali rientranti nel perimetro contrattuale?	
10	Avete adottato misure organizzative interne volte a gestire eventuali violazioni (procedura di data breach ai sensi degli artt. 33 e 34 GDPR)?	
11	Se sì, la procedura “data breach” prevede specifici adempimenti nel caso in cui la violazione di sicurezza riguardi dati personali trattati in qualità di Responsabile del trattamento e, in particolare, obblighi di comunicazione immediata verso il Titolare del trattamento?	
12	Avete un indirizzo e-mail o call center dedicato dove possono essere segnalate violazioni dei dati personali (procedura di data breach ai sensi degli artt. 33 e 34 GDPR)?	

13	Avete adottato misure per rilevare e riscontrare istanze degli interessati finalizzate all'esercizio dei diritti previsti negli art. 15-22 GDPR? Tali misure prevedono specifici obblighi per il caso in cui le richieste riguardino dati personali trattati in qualità di responsabili del trattamento? In particolare, è previsto un obbligo di segnalazione immediata al Titolare e di collaborazione con questo per l'evasione delle richieste?	
14	Disponete di misure tecniche in grado di consentire la cancellazione, la rettifica, l'aggiornamento, la limitazione del trattamento e la portabilità dei Dati personali su richiesta del Titolare e/o al termine del contratto intercorrente con lo stesso?	<i>[In questo caso, si prega di descrivere a/ e misura/e adottate]</i>
15	Contate di servirvi di Sub-Responsabili per la fornitura dei servizi in perimetro contrattuale? Si prega produrre elenco dei Sub-Responsabili aggiornato alla data di compilazione della presente Checklist ai fini dell'accettazione da parte del Titolare.	
16	Avete verificato (e verificate almeno una volta all'anno) l'adeguatezza delle misure tecniche e organizzative di ciascun Sub- Responsabile autorizzato, attraverso la presente Checklist?	
17	Ciascun Sub-Responsabile viene nominato sulla base di un atto il cui contenuto è sostanzialmente conforme a quello intercorrente tra il Titolare ed il Responsabile relativamente a doveri e responsabilità del Sub-Responsabile?	

Sezione C – *Misure tecniche*

Domande		Risposte
1	Disponete di misure tecniche per garantire un adeguato livello di sicurezza all'interno dei sistemi IT utilizzati nel trattamento di dati effettuato in perimetro contrattuale?	<i>[In questo caso, si prega di descrivere la/e misura/e adottate]</i>
2	Disponete di misure tecniche in grado di consentire la restituzione dei dati personali al Titolare o la loro efficace cancellazione/distruzione, su sua richiesta e/o al termine del contratto?	<i>[In questo caso, si prega di descrivere la/e misura/e adottate]</i>
3	Gli accessi delle persone autorizzate al trattamento ai sistemi IT sono protetti da ID e password personali?	
4	La password che ogni autorizzato al trattamento utilizza per accedere ai sistemi IT in perimetro contrattuale è formata da almeno 8 caratteri, non facilmente riferibile all'autorizzato (cioè diversa dalla sua password di accesso) e modificata quando usata per la prima volta e ogni 3 mesi?	<i>[In questo caso, è possibile anche indicare eventuali diverse best practice seguite nella gestione delle credenziali di accesso ai sistemi IT]</i>

5	Le persone autorizzate al trattamento utilizzano account personali e non condivisi per accedere ai dati personali?	
6	Disattivate le credenziali di autenticazione che non vengono utilizzate da almeno 6 mesi?	
7	I profili di accesso ai sistemi IT vengono riesaminati almeno una volta all'anno per verificare che siano corretti, secondo un principio di profilazione degli accessi che tenga conto del ruolo e delle responsabilità di ciascun utente/autorizzato al trattamento?	
8	Le credenziali di accesso sono disattivate quando l'autorizzato al trattamento non ha più diritto di accedere ai dati personali (ad esempio, per cessazione del rapporto di lavoro o cambio di mansione)?	
9	L'accesso da remoto (da reti esterne) agli ambienti che trattano dati personali è protetto mediante autenticazione a più fattori?	
10	Avete adottato misure volte a mitigare gli effetti negativi per gli interessati in caso di violazione dei dati personali? (es. pseudonimizzazione, crittografia, visibilità dei dati personali limitata al solo set di informazioni necessario per le singole attività di elaborazione).	<i>[In questo caso, si prega di indicare tali misure]</i>
11	Avete in atto una procedura di emergenza e di business continuity da seguire in caso di violazione dei dati personali?	<i>[In questo caso, si prega di descrivere tale procedura o allegarla alla presente checklist]</i>
12	Con che frequenza è effettuato il backup dei sistemi in perimetro contrattuale?	
13	I sistemi antivirus e firewall sono aggiornati regolarmente? Con che frequenza?	
14	I sistemi IT mediante i quali vengono trattati i dati personali in perimetro contrattuale sono sottoposti, almeno una volta all'anno, a penetration test e/o vulnerability assessment?	
15	Avete in essere altre procedure che vengono regolarmente eseguite al fine di verificare l'adeguatezza delle misure di sicurezza volte a proteggere l'accesso ai dati personali?	<i>[In questo caso, si prega di descrivere tale procedura o allegarla alla presente checklist]</i>
16	Adottate sistemi di avviso in caso di trasferimento di grandi quantità di dati personali, violazioni dei dati personali, accessi sospetti o attacchi informatici?	
17	Tutti i supporti cartacei contenenti i dati personali in perimetro contrattuale sono conservati in armadi chiusi?	
18	L'accesso ai luoghi in cui vengono conservati i dati personali viene controllato tramite un sistema di badge o qualsiasi altra forma di controllo?	

19	I documenti cartacei e i supporti magnetici/ottici (ad es. dischi rigidi, DVD, CD, smart card, chiavette USB) vengono distrutti o resi inutilizzabili per garantire che i dati e le informazioni in essi contenuti non possano essere ricostruiti e/o utilizzati (anche parzialmente) da terze parti non autorizzate? I documenti cartacei vengono fisicamente distrutti prima di essere cestinati attraverso dispositivi specifici quali distruggi documenti?	
20	Avete adottato misure volte a prevenire la lettura, la copia, la modifica o la cancellazione non autorizzate di dati personali durante il loro eventuale trasferimento o durante il trasporto di supporti contenenti i dati?	<i>[In questo caso, si prega di descrivere tali misure]</i>
21	L'archiviazione di database/archivi di dati è basata su una classificazione appropriata degli asset, in base al livello di criticità? I database/data storage che vengono utilizzati per la memorizzazione dei dati personali in perimetro contrattuale sono protetti tramite strong encryption?	
22	Per la dismissione degli asset IT sono messe in atto procedure di pulizia sicura al fine di rimuovere tutti i dati personali e/o sovrascrivere in modo sicuro prima dello smaltimento o del riutilizzo dello strumento?	
23	Firewall e router sono configurati al fine di limitare il traffico, in entrata e in uscita, da reti "non attendibili" (inclusi wireless) ed i sistemi? È negato tutto il resto del traffico ad eccezione dei protocolli necessari all'ambiente che tratta dati personali?	
24	I firewall delle applicazioni sono configurati davanti ai server Web appartenenti all'ambiente che tratta dati personali, al fine di verificare e convalidare il traffico che è diretto al server? Qualsiasi servizio o traffico non autorizzato viene bloccato e viene generato un avviso?	
25	I dati di produzione sono consentiti e limitati solo agli ambienti di produzione. In casi eccezionali e con le approvazioni necessarie, gli ambienti di test e di sviluppo possono elaborare dati personali (reali) nella misura in cui siano protetti come gli ambienti di produzione. Gli ambienti di test e di sviluppo, così come quelli di pre-produzione utilizzano dati resi anonimi?	

26	Protegete i dati personali durante la trasmissione su reti aperte, pubbliche o non attendibili, con l'implementazione della strong cryptography o l'utilizzazione di protocolli sicuri?	
27	Sono utilizzati strumenti di sicurezza per monitorare e controllare il flusso di dati personali attraverso gli endpoint e verso le reti esterne?	
28	L'accesso agli ambienti di produzione contenenti dati personali e in generale l'accesso ai sistemi contenenti dati personali del Titolare del trattamento sono monitorati e loggati al fine di tracciare l'accesso dell'utente Amministratore di Sistema che accede ai dati personali?	
29	Le registrazioni (access log) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al rispetto della normativa?	
30	Le registrazioni comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate e sono conservate per un congruo periodo, non inferiore a sei mesi?	
31	Verificate il possesso da parte degli AdS dei requisiti di affidabilità e competenza tecnica?	
32	Sono stati comunicati al Titolare del trattamento i nominativi degli AdS nominati dal Responsabile?	
33	PRIVACY BY DESIGN: In caso di fornitura di software e/o APP, viene garantita la conformità privacy by design prevista dal GDPR? Indicare la conformità	
34	Possedere certificazioni (ISO 9001 – 27001 – 27701 - altro)?	<i>[In questo caso, si prega di specificare quali, la data di conseguimento, l'ente certificatore e la data di scadenza]</i>

Firma del Legale Rappresentante del Responsabile:

Data _____

Nome: _____

Firma: _____

All. 5

**Attività di assistenza
su interfacciamento a
piattaforma crediti formativi di CNAPPC**

Indice documento.

1	Premessa	3
2	Contesto operativo	3
3	Oggetto dell'offerta	3
4	Condizioni di fornitura	3
4.1	Trattamento dei dati personali	3
4.2	Riservatezza delle informazioni	4
5	Condizioni economiche e contrattuali	4
5.1	Durata contrattuale	4
5.2	Prezzi.....	4
5.3	Modalità di fatturazione e di pagamento importi dovuti	4
5.4	Clausola risolutiva espressa	4
5.5	Nota di riservatezza	4
5.6	Foro competente	4
5.7	Note	4

1 Premessa

Didanet, nell'ambito delle attività di sviluppo relative alla piattaforma di gestione dei crediti formativi in uso al CNAPPC e agli Ordini territoriali, offre un servizio di consulenza relativamente a esigenze specifiche legate al progetto. La piattaforma GCFP prevede l'esistenza di due ambienti, uno di Certificazione e uno di Esercizio. L'ambiente di Certificazione ha lo scopo di testare le implementazioni senza il rischio di compromettere i dati di produzione. L'ambiente di Esercizio contiene dati reali e rappresenta il punto di destinazione per le implementazioni, una volta che le stesse siano state collaudate. Didanet si impegna a mantenere e manutene entrambi gli ambienti in modo da fornire un completo set di configurazioni utili alle implementazioni dei vari Ordini. In pieno accordo fra il CNAPPC e Didanet, si è deciso di mettere a disposizione l'ambiente di Certificazione GCFP agli Ordini che abbiano fatto richiesta di impiegare il servizio di integrazione GCFP-API. Per accedere al servizio GCFP-API saranno necessarie delle attività di configurazione degli accessi per i fornitori degli Ordini, attività che saranno imputate al CNAPPC nell'ambito del contratto di servizio esistente. La resa disponibilità degli ambienti potrà comportare delle attività di supporto ai fornitori degli Ordini per l'impiego delle GCFP-API, attività che saranno erogate da Didanet nell'ambito del presente accordo, stipulato tra Didanet e gli Ordini o loro Fornitori.

2 Contesto operativo

La procedura di attivazione dell'accesso al sistema GCFP-API è normata dal seguente processo:

1. gli Ordini interessati inviano la modulistica predisposta, compilata e firmata al CNAPPC;
2. il CNAPPC verifica che i moduli siano completi e corretti e inoltra le informazioni di competenza al gestore del servizio (Didanet) per attivare l'accesso al sistema di Certificazione
3. il gestore del servizio conferma l'attivazione tramite una comunicazione inviata al CNAPPC e le credenziali di accesso inviate direttamente all'Ordine;
4. il fornitore dell'Ordine opera gli sviluppi in ambiente di Certificazione;
5. il fornitore comunica all'Ordine di aver collaudato la propria soluzione in Certificazione;
6. l'Ordine comunica al CNAPPC la volontà di passare in Esercizio la soluzione del proprio fornitore;
7. il CNAPPC comunica il passaggio in Esercizio dell'utenza già indicata al punto (3) e il gestore comunica la password di accesso all'ambiente di Esercizio all'indirizzo e-mail dell'Ordine;
8. dopo un periodo di 5 giorni lavorativi dal passaggio in Esercizio l'accesso all'ambiente di Certificazione viene chiuso automaticamente;
9. l'Ordine potrà chiedere un nuovo accesso all'ambiente di Certificazione ripetendo la presente procedura, per lo stesso o per un altro fornitore. In caso di stesso fornitore le credenziali (nome utente) rimangono invariate.

3 Oggetto dell'offerta

Con la presente offerta si rendono disponibili figure specializzate, competenti specificatamente rispetto alla piattaforma in uso agli Ordini, in grado di operare sulla stessa o fornire servizi di consulenza rispetto ad attività svolte da terzi. L'attività si svolgerà in due sessioni di 4 ore, svolte da remoto, nelle quali specialisti forniranno tutte le informazioni di dettaglio necessarie all'interfacciamento al sistema GCFP-API.

4 Condizioni di fornitura

4.1 Trattamento dei dati personali

In relazione alle attività connesse all'esecuzione del presente Contratto, le Parti si conformano al Regolamento 2016/679/EU (Regolamento generale sulla protezione dei dati) e alle ulteriori disposizioni normative vigenti in materia di protezione dei dati personali (d'ora in avanti congiuntamente "Normativa sul trattamento dei dati personali applicabile"). Le Parti, ognuna per quanto di competenza, si impegnano a

mantenersi reciprocamente indenni da ogni contestazione, azione o pretesa avanzate nei loro confronti da parte degli interessati e/o di qualsiasi altro soggetto e/o Autorità a seguito di eventuali inosservanze al suddetto Codice.

Ove necessario, sarà esclusiva cura del cliente, in ottemperanza agli obblighi di cui alla normativa sul trattamento dati personali applicabile, quale Titolare del trattamento fornire ai propri utenti un'informativa adeguata e completa circa le modalità e finalità del trattamento dei loro dati, connesso alla fornitura del Servizio, oggetto delle presenti Condizioni.

4.2 Riservatezza delle informazioni

Didanet e il Cliente garantiscono reciprocamente che il proprio personale e il personale di ditte da esse incaricate, tratteranno come riservata ogni informazione della quale venissero a conoscenza durante od in relazione ad ogni attività inerente all'esecuzione del Contratto.

5 Condizioni economiche e contrattuali

5.1 Durata contrattuale

Il presente accordo ha la validità del tempo necessario all'esecuzione delle attività preventivate.

5.2 Prezzi

Attività	Costo
8 ore distribuite su due sessioni da 4 ore per consulenza a interfacciamento a sistema GCFP-API	700€
Slot di 4 ore aggiuntive	350€

Tutti i prezzi sono da intendersi al netto dell'iva

5.3 Modalità di fatturazione e di pagamento importi dovuti

La fatturazione dei costi è prevista 50% alla firma dell'offerta e 50% al termine delle due sessioni di consulenza. Il pagamento delle fatture è previsto rimessa diretta a vista fattura a mezzo bonifico bancario.

5.4 Clausola risolutiva espressa

In tutti i casi di inadempimento delle obbligazioni di cui agli Art. 4 e 5 del presente contratto, DIDANET avrà la facoltà di risolvere il presente contratto ai sensi dell'art.1456 c.c., senza essere tenuta a restituire quanto dal Cliente pagato in anticipo per importi e/o servizi non ancora usufruiti, fatta salva, in ogni caso, azione di rivalsa e risarcimento per gli ulteriori danni subiti.

5.5 Nota di riservatezza

Tutte le informazioni contenute nel presente documento sono da considerarsi strettamente confidenziali e riservate, di proprietà di Didanet Srl. Esse sono disponibili esclusivamente per le persone o società a cui è intestato o destinato il documento. Le informazioni possono essere utilizzate da queste persone esclusivamente al fine della trattativa e all'esecuzione del progetto. Il cliente e destinatario del documento si impegna a non divulgare le informazioni a terzi. Con la presente si notifica che qualsiasi divulgazione, distribuzione o copia delle informazioni contenute nel documento è da considerarsi non autorizzata ed espressamente vietata.

5.6 Foro competente

Per le controversie che dovessero insorgere nell'interpretazione, esecuzione e validità del presente, sarà competente in via esclusiva il Foro di Venezia.

5.7 Note

La presente offerta rimane valida fino al giorno XX XX XXXX. Per l'accettazione è necessario procedere con la firma e il timbro del presente documento e l'invio via PEC a didanetsrl@itapec.eu allegando copia di un documento d'identità del firmatario.