Allegato

Sicurdata Srl
Via E.Codignola, 10/a
50018 Scandicci (FI)

Supporto in materia di sicurezza nel trattamento del dato

(in conformità al Regolamento 679/2016/UE)

Offerta Economica

Ns. rif.: Nr. 00183/2021_oe del 12.11.2021

COMUNE DI PALAU

C.A. Settore Affari Generali

Spett.le
Sicurdata Srl
Via E. Codignola, 10/a
50018 Scandicci (FI)

Oggetto: **Contratto di individuazione del Responsabile del Trattamento dei Dati ai sensi e per gli effetti dell'art. 28 del Regolamento Europeo 27 aprile 2016, n.679 ("GDPR").**

_____ con sede legale in _____ iscritta nel Registro delle Imprese di _____ - rappresentata dal proprio Amministratore Delegato pro-tempore, in forza dei poteri al medesimo conferiti, in qualità di Titolare del trattamento dati, ai sensi dell'art. 4 del Regolamento UE 2016/679 (GDPR), di seguito anche *Data Controller/Titolare*

e

Sicurdata Srl, con sede legale in Via Ernesto Codignola, 10/a – Scandicci (FI), iscritta nel Registro delle Imprese di Firenze, rappresentata dal proprio Legale Rappresentante, in forza dei poteri al medesimo conferiti, di seguito anche *Data Processor/Responsabile*

PREMESSO CHE:

- in forza del rapporto consulenziale in ambito Data Protection & E-Privacy esistente tra le Parti, **DATA PROCESSOR** potrebbe accedere e trattare per conto di **DATA CONTROLLER** alcune informazioni necessarie per eseguire le attività attribuite all'incarico ricevuto;

- per trattamento si intende "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la co nservazione, 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";

- il Responsabile dichiara e garantisce di possedere competenza e conoscenze tecniche in relazione alle finalità e modalità delle operazioni di trattamento, alle misure di sicurezza da adottare a garanzia della riservatezza, completezza ed integrità dei dati trattati, nonché alla normativa applicabile in materia di tutela dei dati personali;

- il Data Controller definisce, nel rispetto dell'art 28 del GDPR, i seguenti elementi identificativi del trattamento dei dati affidati al Responsabile:

natura e finalità del trattamento	*Il trattamento è necessario per dare esecuzione al contratto e le finalità di trattamento sono definite dal Titolare del trattamento*
tipi di dati personali trattati	*Dati personali comuni* *Dati appartenenti a categorie particolari*
categorie di interessati di cui vengono trattati i dati	*Clienti, Fornitori, Dipendenti, consumatori, associati, aderenti, etc…*

- alla luce delle verifiche documentali effettuate, possiede l'esperienza, la capacità,

l'affidabilità e fornisce idonee garanzie del pieno rispetto delle disposizioni vigenti in materia di trattamento dati, ivi compreso il profilo della sicurezza in relazione alle finalità e alle modalità delle operazioni di trattamento nonché alle garanzie di tutela dei diritti dell'interessato;

- le Parti intendono regolare, con il presente atto, i loro reciproci rapporti in tema di disciplina del trattamento dei dati personali.

Tutto ciò premesso, che costituisce parte integrante del presene atto, le Parti convengono e stipulano il seguente

CONTRATTO di NOMINA del RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

OGGETTO|MATERIA

Con la stipula del presente atto, ai sensi dell'articolo 28 del Regolamento UE 2016/679 (GDPR), il Titolare designa **DATA PROCESSOR** "Responsabile" delle operazioni di trattamento dei dati personali affidati. In virtù di tale nomina e del rapporto contrattuale intercorrente tra le Parti, il Responsabile è autorizzato al trattamento dei dati individuati per natura e finalità, tipologia e per categorie di interessati a cui si riferiscono e strettamente pertinenti alle attività svolte per conto di **DATA CONTROLLER** e per le finalità previste dal Titolare del trattamento.

OBBLIGHI DEL RESPONSABILE: La sottoscrizione del presente atto vincola il Responsabile del trattamento al Titolare del trattamento e fa sorgere in capo al Responsabile una serie di obblighi specificamente individuati in apposita e separata clausola che segue il presente documento (**Allegato A**).

MISURE DI SICUREZZA E VIOLAZIONE DEI DATI: Il Responsabile è tenuto a mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio in merito al trattamento dei dati effettuato (art. 32 GDPR) meglio precisate nell'**Allegato B** del presente documento.

DECORRENZA – DURATA - CESSAZIONE DEL TRATTAMENTO

Il ruolo e le competenze assegnate al Responsabile del trattamento con il presente atto, hanno la medesima durata ed efficacia del Contratto intercorrente tra le Parti e pertanto si intendono tacitamente rinnovate ogni anno fino alla cessazione del Contratto stesso o fino alla revoca da parte del Titolare.

Dopo il completamento del trattamento per conto del Titolare, il Responsabile deve, su istruzioni del Titolare del trattamento, restituire o cancellare i dati personali, e le relative copie esistenti, salvo che non siano previste specifiche e differenti politiche di conservazione dei dati (anche in relazione alle categorie di dati trattati) a norma del diritto dell'Unione o degli Stati membri cui è soggetto il Responsabile del trattamento. In entrambi i casi il Responsabile deve rilasciare contestualmente un'attestazione scritta che presso lo stesso non esiste alcuna copia dei dati personali trattati in nome e per conto del Titolare del trattamento.

È fatto divieto al Responsabile del trattamento di avvalersi di soggetti Terzi ai fini del trattamento di dati personali per conto del Titolare del trattamento oggetto del mandato senza la relativa autorizzazione da parte di quest'ultimo e salvo l'adempimento di un obbligo della legge italiana o dell'Unione europea, che andrà comunque comunicato al Titolare del trattamento, laddove tale comunicazione non sia vietata dalla legge. Nel caso

in cui il Responsabile si serva di sub-fornitori per svolgere le attività strettamente necessarie all'esecuzione dei servizi richiesti dal Titolare, che comportino trattamento di dati personali del Titolare, lo stesso è autorizzato solo se il Responsabile si impegna a selezionare sub-fornitori tra soggetti che per esperienza, capacità e affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso il profilo relativo alla sicurezza; nonché a stipulare specifici accordi scritti con i sub-fornitori a mezzo dei quali il Responsabile specifichi analiticamente i loro compiti e imponga a tali soggetti di rispettare i medesimi obblighi, con riferimento alla disciplina sulla protezione dei dati personali imposta dal Titolare sul Responsabile. A ciò si aggiunga che il Responsabile comunque si impegna a garantire circa il rispetto da parte degli eventuali sub-fornitori di tutti gli obblighi con riferimento alla disciplina sulla protezione dei dati personali, imposti dal Titolare sul Responsabile, manlevare e tenere indenne il Titolare da qualsiasi danno, pretesa e/o sanzione possa derivare al Titolare medesimo dalla mancata osservanza di tali obblighi e più in generale dall'applicabile normativa sulla tutela dei dati personali da parte dei sub-fornitori. La lista dei sub-fornitori nominati è disponibile presso la sede del Data Processor ed è possibile richiederne una copia scrivendo a privacy@opendata.it.

Le comunicazioni tra le parti, ai fini del presente incarico, dovranno avvenire:
- per il Titolare, _____
- per il Responsabile, a privacy@opendata.it

Il corrispettivo per il presente incarico di Responsabile Esterno del trattamento rimane ad ogni effetto ricompreso nel compenso complessivo pattuito per la fornitura dei servizi già in essere e disciplinati nel contratto.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Con l'occasione, **DATA CONTROLLER** ricorda l'importanza delle prescrizioni di legge in materia di trattamento dei dati personali, nonché il fatto che la violazione di dette normative può comportare responsabilità sia civili che penali per il Titolare e per il Responsabile, con possibile applicazione di sanzioni amministrative e pecuniarie, ai sensi degli artt. 82, 83 e 84 GDPR.

***

Si prega, dunque, di voler cortesemente restituire copia della presente sottoscritta per accettazione.

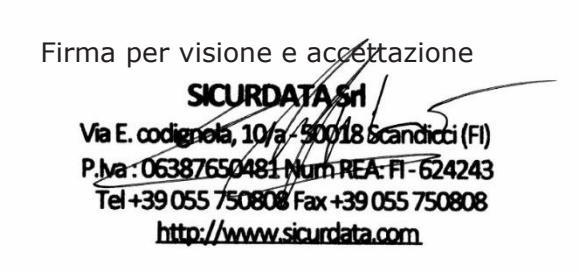
Luogo e data:

Il titolare
Timbro e firma del legale rappresentante

ACCETTAZIONE NOMINA

Il sottoscritto Agostino Oliveri, legale Rappresentante di **Sicurdata Srl**, accetta la presente nomina nei contenuti, limiti, obblighi ed istruzioni in essa indicati.

Firma per visione e accettazione



ALLEGATI:

- *Allegato A.* Obblighi del Responsabile del trattamento designato.
- *Allegato B.* Misure di Sicurezza e Violazione dei dati.

ALLEGATO A. Obblighi del Responsabile del trattamento designato. (art. 28 e Considerando 81 e ss del Regolamento EU 2016/679)

In virtù dell'atto che vincola il Responsabile designato al Titolare del trattamento, sorgono in capo al Responsabile una serie di obblighi.

1. **Rispetto delle istruzioni impartite dal/i Titolare/i:** Il Responsabile deve assistere e coadiuvare il Titolare nella corretta gestione delle operazioni di trattamento che dovranno esser effettuate nel pieno rispetto degli obblighi previsti dal GDPR. A tale proposito, il Responsabile deve trattare i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del trattamento; in tal caso, il Responsabile deve informare il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
2. **Riservatezza**: Il Responsabile deve assicurare per se stesso e per le persone, da lui o dal Titolare del trattamento autorizzate al trattamento dei dati personali, piena riservatezza rispetto alle operazioni di trattamento effettuate.
   Sarà cura del Responsabile, qualora lo reputasse opportuno, vincolare le persone autorizzate al trattamento dei dati al segreto mediante un adeguato obbligo legale di riservatezza, anche per il periodo successivo all'estinzione del rapporto di lavoro intrattenuto con il Responsabile, in relazione alle operazioni di Trattamento da essi eseguite.
3. **Conformità a leggi e regolamenti applicabili:** Il Responsabile è tenuto ad uniformarsi alle disposizioni del GDPR e più in generale, di ogni altra disposizione normativa, nazionale e sovranazionale, in materia di trattamento dei dati personali attualmente in vigore o che in futuro vengano a modificare, integrare o sostituire l'attuale disciplina, nonché dei provvedimenti dell'Autorità Garante competente e delle linee guida adottate dall'European Data Protection Board.
4. **Misure di sicurezza:** Il Responsabile è tenuto a mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio in merito al trattamento dei dati effettuato (art. 32 GDPR). Si veda Allegato B. Misure di sicurezza e Violazione dei dati;
5. **Audit:** Il Responsabile del trattamento deve riferire al Titolare, almeno annualmente e ogni volta che riceve specifica richiesta in tal senso, sui dettagli relativi all'adempimento di quanto disposto dal presente contratto nonché dalla normativa privacy, o attraverso relazioni scritte o attraverso compilazione di check list che verranno fornite. Inoltre, il Responsabile deve contribuire alle attività di revisione, comprese le ispezioni, e ad informare prontamente il Titolare del trattamento di ogni questione rilevante ai fini del presente mandato, quali a titolo indicativo:
   - Istanze di interessati;
   - Richieste del Garante;
   - Esiti delle ispezioni;
   - Violazioni del GDPR o di altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati, o la messa in pericolo della riservatezza, della completezza o dell'integrità dei dati personali.
6. **Persone autorizzate al trattamento:** Il Responsabile si avvale di persone autorizzate al trattamento dei dati che operano sotto la sua responsabilità, in quanto deputati alle operazioni di Trattamento, e alle quali fornisce specifiche istruzioni scritte (salvo che il diritto dell'Unione o degli Stati membri non richieda diversamente, art. 29 GDPR). È compito del Responsabile designato vigilare sulla corretta esecuzione delle istruzioni impartite (art. 4.10 GDPR).
7. **Provvedimento a carattere generale dell'Autorità Garante Privacy del 27 Novembre 2008:** Se applicabile, il Responsabile garantirà al Titolare del trattamento che ciascun incaricato amministratore di sistema accederà con proprio utente e propria password. Con l'accettazione di questa nomina si impegna a nominare individualmente - ai sensi del Provvedimento a carattere generale dell'Autorità Garante Privacy del 27 Novembre 2008 (G.U. N. 300 Del 24 dicembre 2008), cosi come modificato dal Provvedimento a carattere generale dell'Autorità Garante Privacy del 25

giugno 2009 (G.U. N. 149 Del 30 giugno 2009), gli incaricati della propria struttura che rivestono il ruolo di Amministratori del Sistema informativo. La designazione quale Amministratore di Sistema deve essere individuale e recare l'elencazione anali tica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

8. **Registrazione degli accessi:** qualora nello svolgimento delle attività di cui al presente contratto, il Responsabile operi su sistemi allocati presso propria sede e/o presso sedi di soggetti terzi (diversi dal Titolare del trattamento), il Responsabile assicura l'adozione di sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi. Il Titolare del trattamento può richiedere di ricevere copia delle predette registrazioni.
9. **Sub-responsabile:** Il Titolare del trattamento autorizza il Responsabile del trattamento, **DATA PROCESSOR**, a ricorrere ad un altro Responsabile (di seguito "Sub-responsabile") per l'esecuzione di specifiche attività di trattamento. Il Responsabile informa il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri Responsabili, alle quali il Titolare del trattamento conserva il diritto di opporsi. Al "Sub-responsabile" sono imposti, con specifico atto sottoscritto, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto che lega il Titolare e il Responsabile del trattamento. Il "Sub-responsabile" è tenuto ad: osservare, valutare e organizzare la gestione del trattamento dei dati personali e la loro protezione (mettendo in atto tutte le misure tecniche ed organizzative adeguate per assicurare un livello di sicurezza adeguato al rischio derivante dal trattamento dati effettuato) affinché questi siano trattati in modo lecito e pertinente e nel rispetto della normativa vigente. Qualora il "Sub-responsabile" del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del "Sub-responsabile" anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" *(*art. 82. 1 e 82. 3 GDPR).
10. **Registro dei Trattamenti:** Ove applicabile, il Responsabile deve tenere un Registro delle attività di trattamento svolte sotto la propria responsabilità in nome e per conto del Titolare del trattamento (art. 30 GDPR). Il Registro, anche in formato elettronico, deve contenere tutta una serie di informazioni, che il Responsabile raccoglie anche interfacciandosi con i vari uffici o unità interne e/o esterne all'azienda, che trattano dati personali per conto del Titolare. In particolare:
    - il nome e i dati di contatto del Responsabile del trattamento;
    - le categorie dei trattamenti effettuati per conto di ogni Titolare;
    - i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale;
    - una descrizione delle misure tecniche adottate.

    Il Responsabile del trattamento deve mettere il Registro a disposizione dell'Autorità di controllo, se questa ne fa richiesta, affinché possa fungere da strumento per il monitoraggio dei trattamenti effettuati (Considerando 82 GDPR).
11. **Esercizio dei diritti dell'interessato:** Il Responsabile, dovrà informare tempestivamente e per iscritto il Titolare del trattamento, della ricezione di eventuali richieste degli interessati, avanzate ai sensi degli artt. da 15 a 22 del GDPR, in merito, tra l'altro, alle finalità e alle modalità del trattamento, all'origine dei dati, all'aggiornamento, alla rettificazione, cancellazione, alla portabilità e limitazione dei dati od opposizione al trattamento (compresa la profilazion e), o al fine di revocare il consenso prestato e/o proporre reclamo al Garante per la protezione dei dati personali.

    In particolare, il Responsabile è tenuto a:
    - coordinarsi a tal fine con le funzioni aziendali preposte dal Titolare alle relazioni con i soggetti interessati;

- darne tempestiva comunicazione scritta al Titolare allegando copia della richiesta;
- accertare l'identità del richiedente per verificare la legittimità della richiesta;
- attivare le dovute procedure atte a dare seguito alle richieste per l'esercizio dei diritti degli interessati, senza ingiustificato ritardo, e comunque, al più tardi entro un mese dal ricevimento delle richiesta stesse, ai sensi dell'art. 12 GDPR.

12. Altri adempimenti: il Responsabile del trattamento è tenuto altresì a:

- cooperare con l'Autorità di Controllo quando richiesto;
- supportare l'attività svolta dal DPO (Data Protection Officer – Responsabile della Protezione dei Dati) per conto del Titolare del trattamento, se nominato (artt. 37,38 GDPR);
- designare per iscritto un Rappresentante che lo rappresenti nell'Unione, se il Responsabile non è stabilito nell'UE e ricorrano i presupposti di cui all'art. 27 GDPR.

ALLEGATO B. Misure di Sicurezza e Violazione dei dati

(artt.32 e ss e Considerando 74-77, 83 e ss del Regolamento EU 2016/679 – GDPR)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Responsabile del trattamento deve mettere in atto misure tecniche e organizzative adeguate per assicurare un livello di sicurezza adeguato al rischio, previste dall'art. 32 GDPR, che comprendono, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Tali misure devono assicurare un elevato livello di sicurezza. Nella valutazione del rischio per la sicurezza dei dati il Responsabile del trattamento deve tenere in considerazione i rischi presentati dal trattamento dei dati personali come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale. Il Responsabile del trattamento, se necessario e su richiesta, dovrà altresì assistere il Titolare del trattamento nella redazione del "DPIA" (*Data Protection Impact Assessment),* contenente la valutazione sulla particolare probabilità e gravità del rischio inerente alle operazioni di trattamento da effettuare (tenuto conto della natura, dell'ambito di applicazione, del contesto, delle finalità e delle fonti di rischio) e sulle misure tecniche ed organizzative da adottare al fine di attenuare tale rischio assicurando la protezione dei dati personali e la conformità al GDPR. Se del caso, il Responsabile dovrà richiedere in merito un parere al DPO (*Data Protection Officer*), se nominato (art.35 e C.90 GDPR).

Violazione dei dati. Se dovesse venire a conoscenza di una violazione dei dati personali (*Data Breach*), il Responsabile, senza ingiustificato ritardo, deve informare per iscritto il Titolare del trattamento affinché possa procedere, se del caso, a notificare la violazione all'autorità di controllo competente (art.33 GDPR) e, qualora la violazione dei dati personali in questione dovesse essere suscettibile di presentare un elevato rischio per i diritti e le libertà delle persone fisiche, il Titolare del trattamento provvederà a darne comunicazione all'interessato (art.34 GDPR).

Il Responsabile deve coadiuvare il Titolare del trattamento nella redazione di specifiche procedure che consentono di individuare prontamente le violazioni dei dati subite (Data Breach) e le relative procedure di risposta attraverso l'elaborazione di una specifica policy. La suddetta policy deve includere, tra le altre cose:

- le linee guida per valutare le violazioni di dati subite al fine individuare quelle che sono suscettibili di presentare un elevato rischio per i diritti e le libertà delle persone
- fisiche e che dunque dovranno essere notificate all'Autorità di controllo competente;
- le linee guida sulla scelta delle informazioni che saranno rese disponibili all'interessato dal Titolare del trattamento attraverso la comunicazione della violazione, se dalla valutazione precedentemente effettuata, fosse risultata suscettibile di presentare rischi elevati per i diritti e le libertà dell'interessato.
- Il Responsabile dovrà aiutare il Titolare del trattamento a documentare per iscritto qualsiasi

violazione di dati subita, le circostanze ad essa relative, le conseguenze e i provvedimenti adottati per porvi rimedio.

Nello specifico dovranno essere documentati:

- la natura della violazione dei dati personali compresi, 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;
- il nome e i dati di contatto del DPO (se nominato) o di altro punto di contatto presso cui l'Autorità di controllo competente potrà ottenere maggiori informazioni;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizioni delle 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 attenuare i possibili effetti negativi.

Tale documentazione dovrà essere resa disponibile all'Autorità di controllo competente attraverso la procedura di notifica della violazione dei dati (*Data breach)* prevista dall'art. 33 comma 3.

Firma per accettazione degli allegati A e B

***Oggetto**: informativa sul trattamento dei Vostri dati personali ai sensi dell'articolo 13 del Regolamento UE 679/2016 (in inglese General Data Protection Regulation e, di qui in avanti "GDPR") - Versione ottobre 2021 (La presente informativa sarà riesaminata e adeguata, se necessario, in caso di adeguamento normativo).*

Vi informiamo che, per l'instaurazione e l'esecuzione dei rapporti contrattuali con Voi in corso, la nostra organizzazione entrerà in possesso di dati riferibili alla Vostra struttura, acquisiti anche verbalmente, direttamente o tramite terzi, qualificati come personali dal GDPR 679/2016.

La GDPR prevede che chi effettua trattamenti di dati personali sia tenuto ad informare il soggetto interessato, su quali dati vengano trattati e su taluni elementi qualificanti il trattamento. Esso deve avvenire con correttezza liceità e trasparenza, tutelando la riservatezza ed i diritti degli interessati.

Per tale motivo Vi forniamo le seguenti informazioni:

1. Titolare del trattamento

1.1. Titolare del trattamento è **Sicurdata Srl**, i cui dati anagrafici sono riportati nell'intestazione della presente lettera.

1.2. Dati di contatto del titolare: a) indirizzo e-mail: info@opendata.it; b) indirizzo PEC: sicurdatasrl@pec.pec-opendata.com; c) numero di telefono: 055750808

2. Natura dei dati trattati

2.1. Il trattamento è relativo ai dati anagrafici e fiscali, nonché i dati di natura economica, che sono necessari per lo svolgimento dei rapporti contrattuali intercorsi e/o intercorrenti e/o che intercorreranno tra Sicurdata S.r.l. e la vostra struttura.

2.2. I dati potrebbero essere relativi al legale rappresentante ovvero ai referenti della Vostra struttura con cui Sicurdata S.r.l. si interfaccerà durante l'espletamento dei servizi contrattualizzati.

2.2.1. In quest'ultimo caso si prega di fornire la presente informativa anche a tali soggetti.

3. Finalità del trattamento e base giuridica del trattamento, natura del conferimento

3.1. I dati personali potranno essere trattati per le seguenti finalità e in forza delle relative basi giuridiche:

a) Finalità: inserimento delle anagrafiche nei data base informatici aziendali. Base giuridica: art. 6.1 lett. b) GDPR in quanto il trattamento è necessario per erogare il servizio richiesto. Natura del conferimento: necessaria per l'erogazione del servizio contrattualizzato.

b) Finalità: per soddisfare le esigenze contrattuali ed i conseguenti adempimenti degli obblighi legali e contrattuali dalle stesse derivanti e per adempiere agli obblighi previsti dalle norme di legge civilistiche, fiscali, dai regolamenti e dalla normativa comunitaria, compreso la tenuta della contabilità. Base giuridica: art. 6.1 lett. b) GDPR in quanto il trattamento è necessario per erogare il servizio richiesto ed art. 6.1 lett. c) GDPR in quanto il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento. Natura del conferimento: necessaria per l'erogazione del servizio contrattualizzato e, una volta effettuato, i trattamenti descritti dovranno essere effettuati in forza di un obbligo normativo.

c) Finalità: conseguire un'efficace gestione dei rapporti commerciali anche ai fini della tutela del credito. Base giuridica: Art. 6.1 lett. f) GDPR in quanto il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento. Natura del conferimento: una volta conferiti i dati per le finalità relative all'erogazione dei servizi contrattualizzati, gli stessi saranno trattati anche per tale finalità.

d) Finalità: attività di newsletter, finalizzate a tenerla aggiornata sulla materia della privacy, della protezione dei dati ed alle attività strettamente connesse. Base giuridica: il suo consenso ai sensi dell'art. 6.1 lett. a) GDPR. Natura del conferimento: facoltativa e la sua assenza non pregiudica la fruizione dei servizi contrattualizzati.

e) Finalità: offerte commerciali ed iniziative di marketing (in corso e future). Base giuridica: il suo consenso ai sensi dell'art. 6.1 lett. a) GDPR. Natura del conferimento: facoltativa e la sua assenza non pregiudica la fruizione dei servizi contrattualizzati.

f) Finalità: rilevazione della soddisfazione del cliente relativi ai nostri prodotti/servizi. Base giuridica: Art. 6.1 lett. f) GDPR in quanto il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento. Natura del

conferimento: una volta conferiti i dati per le finalità relative all'erogazione dei servizi contrattualizzati, gli stessi saranno trattati anche per tale finalità.

g) Finalità: inviti a manifestazioni ed eventi scientifici. Base giuridica: il suo consenso ai sensi dell'art. 6.1 lett. a) GDPR. Natura del conferimento: facoltativa e la sua assenza non pregiudica la fruizione dei servizi contrattualizzati.

h) Finalità: inserimento del Vostro nominativo nelle nostre referenze e progetti svolti sia su formato cartaceo (brochure) sia su formato elettronico (sito internet istituzionale) solo per il tempo strettamente necessario e legato al rapporto commerciale in essere. Base giuridica: il suo consenso ai sensi dell'art. 6.1 lett. a) GDPR. Natura del conferimento: una volta conferiti i dati per le finalità relative all'erogazione dei servizi contrattualizzati, gli stessi saranno trattati anche per tale finalità.

3.2. In relazione ai trattamenti per i quali è necessario un suo consenso, la informiamo che lo stesso è revocabile in qualsiasi momento (art. 7 GDPR), ma la revoca non pregiudica la liceità del trattamento basata sul consenso prima della revoca stessa.

4. Destinatari dei dati personali

4.1. I dati personali ottenuti nel contesto dei servizi offerti potranno essere trasmessi a:

a) soggetti a cui la comunicazione derivi da un obbligo normativo ovvero sia necessari per la gestione dei servizi erogati e che agiranno in qualità di autonomi titolari del trattamento (a titolo esemplificativo e non esaustivo: Istituti di credito, spedizionieri, etc…);

b) soggetti a cui la comunicazione sia necessaria per l'erogazione dei servizi richiesti e che tratteranno i dati in qualità di responsabili del trattamento ai sensi dell'art. 28 GDPR. Questi sono: a) soggetti che erogano assistenza su software e gestionali; b) fornitore del servizio di *newslettering*; c) soggetti che erogano servizio di hosting per conto di Sicurdata S.r.l. A tali soggetti il titolare ha fornito apposite istruzioni su come effettuare il trattamento dei dati personali per suo conto.

c) soggetti che operano sotto l'autorità del titolare, debitamente autorizzati ed istruiti al trattamento ai sensi dell'art. 29 GDPR.

4.2. L'elenco specifico dei responsabili del trattamento può essere richiesto al titolare del trattamento ad uno dei punti di contatto indicati nella presente informativa.

5. Periodo di conservazione dei dati

5.1. I dati personali trattati per le finalità amministrative e contabili saranno conservati per un periodo di dieci anni, come stabilito dall'art. 2220 c.c.

5.2. I dati personali trattati per l'erogazione dei servizi contrattualizzati e tutti gli adempimenti connessi saranno conservati per un periodo di dieci anni a partire dalla cessazione del rapporto.

5.3. I dati personali trattati in forza del suo consenso saranno conservati fino a che lo stesso non sia revocato, ricordandole che il consenso può essere revocato in qualsiasi momento e che la revoca non pregiudica la liceità del trattamento basata sul consenso prima della revoca stessa.

6. Trasferimento dei dati personali a Paesi Extra-UE

6.1. Non è previsto un trasferimento dei dati personali a Paesi Extra-UE.

7. Diritti dell'Interessato

7.1. Relativamente ai dati personali ottenuti nel contesto dei servizi offerti i soggetti interessati potranno esercitare i seguenti diritti:

a) il diritto di accesso, espressamente previsto dall'art. 15 GDPR;

b) il diritto di rettifica, espressamente previsto dall'art. 16 GDPR;

c) il diritto all'oblio, espressamente previsto dall'art. 17 GDPR;

d) il diritto di limitazione di trattamento quando ricorre una delle ipotesi previste dall'art. 18 GDPR;

e) il diritto a ricevere l'attestazione che le operazioni effettuate a norma degli artt. 16, 17 e 18 GDPR siano state portate a conoscenza di coloro ai quali i dati sono stati comunicati, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato, ai sensi dell'art. 19 GDPR;

f) il diritto alla portabilità dei dati, espressamente previsto dall'art. 20 GDPR;

g) il diritto di opposizione al trattamento dei dati personali, espressamente previsto dall'art. 21 GDPR;

h) il diritto di revoca del consenso in qualsiasi momento, come stabilito dall'art. 7 GDPR.

7.2. Lei ha il diritto di proporre reclamo ad un'autorità di controllo, ai sensi dell'art. 77 GDPR.

7.3. Per esercitare i suoi diritti potrà rivolgersi al titolare del trattamento o al responsabile della protezione dei dati ai punti di contatto indicati nella presente informativa.

Sicurdata Srl

Dati e Consenso al trattamento dei dati personali
da restituire a Sicurdata Srl

Il sottoscritto/La sottoscritta _____ dopo attenta lettura dell'informativa rilasciata ai sensi dell'art 13 GDPR:

☐ esprime il consenso ☐ nega il consenso

Al trattamento finalizzato all'attività di newsletter relative alla materia della privacy, della protezione dei dati ed alle attività strettamente connesse

☐ esprime il consenso ☐ nega il consenso

Al trattamento dei dati personali effettuato con il fine di proporre offerte commerciali ed iniziative di marketing (in corso e future)

☐ esprime il consenso ☐ nega il consenso

Al trattamento dei dati personali effettuato con il fine di proporre inviti a manifestazioni ed eventi scientifici

☐ esprime il consenso ☐ nega il consenso

Al trattamento finalizzato all'inserimento del Vostro nominativo nelle nostre referenze e progetti svolti sia su formato cartaceo (brochure) sia su formato elettronico (sito internet istituzionale) solo per il tempo strettamente necessario e legato al rapporto commerciale in essere

Data e luogo _____

Firma e timbro (cliente) _____

Sicurdata Srl
Via E.Codignola, 10/a
50018 Scandicci (FI)

Supporto in materia di sicurezza nel trattamento del dato

(in conformità al Regolamento 679/2016/UE)

Offerta Economica

Ns. rif.: Nr. 00183/2021_oe del 12.11.2021

COMUNE DI PALAU

C.A. Settore Affari Generali

Sommario

1. INTRODUZIONE 1
1.1 Valutazioni 1
1.2 Aspetti Qualificanti della Proposta 3
1.3 Aspetti Migliorativi della Proposta 3
1.4 Referenze 3
2. SINTESI DELLA PROPOSTA 5
3. COSTI 6
3.1 Nomina Data Protection Officer 6
3.2 Formazione secondo GDPR 679/2016 7
3.3 Supporto SGP come previsto dal GDPR 679/2016 8
4. RIEPILOGO COSTI 9
5. CONDIZIONI DI FORNITURA 10
6. SICURDATA S.R.L. DICHIARA 11
7. TRATTAMENTO DATI PERSONALI 12

Scandicci, 12/11/2021

1. INTRODUZIONE

Scopo del presente documento è quello di illustrare il progetto economico di consulenza per raggiungere gli obiettivi di supporto al mantenimento dei requisiti imposti dal Regolamento UE 679/2016 in materia di trattamento dei dati personali.

Il presente progetto è rivolto a: **COMUNE DI PALAU**

1.1 VALUTAZIONI

A seguito della richiesta pervenuta e delle informazioni ricevute, visto i recenti cambiamenti e modifiche in materia di trattamento dati personali, con la presente si intende offrire un servizio di supporto al mantenimento dei requisiti imposti dal Regolamento UE 679/2016.

Le principali novità introdotte dal Nuovo Regolamento sono:

- Danno Reputazionale e Incauto Affidamento;
- Registri dei trattamenti;
- Principio di trasparenza ed esattezza nella gestione dei dati;
- introduzione della responsabilità solidale;
- introduzione del concetto del privacy by design e privacy by default;
- obbligatorietà del Data Protection Officer;
- introduzione del joint controller;
- diritto all'oblio, in particolar modo per i dati on-line;
- previsione di un consenso chiaro ed inequivocabile;
- i dati genetici e biometrici sono considerati dati sensibili;
- maggiori informazioni sul periodo di conservazione dei dati;
- one stop shop;
- data breach notification;
- previsione di Data Privacy Impact Assessment (DPIA) e dei registri del trattamento;
- codice di condotta e schemi di certificazione Privacy.

Nel REGOLAMENTO EUROPEO entrato in vigore il 24 maggio 2016 e che ha avuto la sua piena applicabilità a partire dal 25 maggio 2018 pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento. Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento. In caso di trattamento illecito dei dati, le Autorità Garanti nazionali potranno imporre sanzioni amministrative che possono arrivare nei casi più gravi sino al 4% del fatturato mondiale annuo dell'impresa o 20 milioni di Euro.

A tal proposito SICURDATA ha creato il **C.C.P. (C**entro **C**ompetenza **P**rivacy**)** composto dalle seguenti competenze professionali:

- Esperti certificati in materia di Data Protection & E-Privacy
- Esperti in Governance Aziendale;
- Esperti in Sistema di Gestione e certificazioni ISO;
- Esperti Legali;
- Esperti certificati in Sicurezza Informatica;
- Esperti certificati in sistemi di Auditing.

La squadra di professionisti del **C.C.P.** è guidata da:

Agostino Oliveri Data Protection Officer e Auditor Certificated

N. di Reg. DPO2833 secondo gli standard UNI 11697:2017 UNI PDR 66:2019

Auditor DataBase & Privacy Management - Num. Reg. EdPsFeA1607014

secondo gli standard PRD UNI EN ISO/IEC 17065:2012

CEO di Sicurdata Srl e Responsabile del C.C.P. di SICURDATA

Esperienza ventennale tecnica e di project management nel campo delle architetture di rete e della sicurezza, computer forensics Cyber Security e gestione degli incidenti, analisi e disegno di basi dati, integrazione di piattaforme software, consulenza procedurale ed organizzativa per l'adeguamento alle normative nazionali ed internazionali in materia di misure di sicurezza informatica (Privacy, Garante AdS, Codice Amministrazione Digitale – Disaster Recovery, ISO 27001) e sicurezza sul lavoro.

Partner of DNV·GL

Partner DNV GL - Business Assurance

Collabora attivamente su diversi progetti di sicurezza con le community di settore fra cui:

- Iscritto come socio sostenitore e coordinatore dell'area di ricerca Legal & Privacy di CSA Italy (Associazione Cloud Security Alliance Italy Chapter)
- Iscritto come socio sostenitore a CLUSIT (Associazione Italiana per la Sicurezza Informatica)
- Referente territoriale area nazionale ASSODPO
- Iscritto al GDL (Gruppo di Lavoro) della Oracle Community for Security
- Membro Contributors at Europrivacy.info

Il DPO Agostino Oliveri ha maturato anche altre esperienze ed è in grado di fornire assistenza, nelle attività di seguito elencate:

1. Adeguamenti in materia di responsabilità amministrativa come previsto dalla legge 231/2001;
2. Piani di Continuità Operativa e Disaster Recovery in conformità dell'art. 50 – bis del Codice di Amministrazione Digitale

3. Conduzione e sostegno verso la compliance aziendale rispetto a dispositivi di Legge o standard internazionali (ISO 9001, ISO/IEC 27001, ISO/IEC 27018 per i servizi in modalità CLOUD COMPUTING, ISO/IEC 20000, ecc.);
4. Adeguamenti in materia di DL. 33/2013 sulla Trasparenza e L. 190/2012 sull'Anticorruzione;
5. Adeguamenti in materia di sicurezza sul lavoro Dlgs. 81/2008;
6. Progetti Formativi

1.2 ASPETTI QUALIFICANTI DELLA PROPOSTA

Elemento essenziale è la diffusione a tutti i livelli dell'organizzazione aziendale dell'abitudine a prevedere il risultato delle proprie azioni in termini di impatto sulla soddisfazione dei clienti gestendo le informazioni in modo corretto e dimostrando la consapevolezza e importanza nella conservazione e utilizzo dei dati dei propri Clienti, fino a generare una sorta di "riflesso condizionato".

Verrà investito parte del tempo dedicato al progetto anche a quest'attività.

Il C.C.P. di SICURDATA offrirà la Sua consulenza applicando il ciclo PDCA (Plan-Do-Check-Act); il punto di partenza è costituito da una diagnosi finalizzata alla individuazione delle aree di debolezza per pianificare le azioni di miglioramento, sperimentarle, verificarle e consolidarle. Proprio per questo e alla luce della recente politica di sensibilizzazione avviata nel vostro settore la consulenza offerta sarà finalizzata al rispetto e adozione delle ***MISURE ADEGUATE*** *come previsto dall'art. 32 del Nuovo Regolamento UE GDPR 679/2016*.

1.3 ASPETTI MIGLIORATIVI DELLA PROPOSTA

La progettazione ed implementazione di un Sistema e Dossier Privacy è una premessa indispensabile per garantire il rispetto dei fattori di Qualità, senza il quale non è possibile conseguire la soddisfazione dei clienti.

Il Sistema e Dossier Privacy ha, inoltre, la possibilità di integrarsi con altri aspetti quali la normativa ambientale, la sicurezza del lavoro, la certificazione della qualità, ecc.

Inoltre il C.C.P. di Sicurdata garantisce e assicura nel tempo il costante miglioramento delle prestazioni, verificandone la coerenza con le necessità/aspettative del Cliente.

1.4 REFERENZE

L'attività erogata dal C.C.P. di SICURDATA Srl si basa su un'esperienza ventennale e certificata da un organismo indipendente accreditato **ACCREDIA** (ex Sincert) al n° **68C**, per la Certificazione di Auditor, Data Protection Officer, Lead Auditor e Privacy Consultant nei vari settori fra cui Privacy, Qualità, Ambiente, Sicurezza e Energia.

Per Accreditamento si intende:

- il "Procedimento con cui un Organismo riconosciuto attesta formalmente la competenza di un organismo o persona a svolgere funzioni specifiche".

L'Accreditamento è una scelta **volontaria** degli Organismi di Certificazione che intendono così impegnarsi nel dare evidenza di una caratteristica in più per quanto riguarda la correttezza, la trasparenza e la professionalità della loro attività. Grazie alla partecipazione degli Enti di Accreditamento nazionali (per l'Italia Accredia) ad Organizzazioni internazionali – quali **EA** (European Cooperation for Accreditation) a livello europeo e **IAF** (International Accreditation Forum) a livello internazionale – e alla sottoscrizione degli Accordi di Mutuo Riconoscimento (**MLA**) gestiti da tali Organizzazioni, **le certificazioni rilasciate da Organismi accreditati da Enti di Accreditamento firmatari degli Accordi MLA risultano valide e credibili, nonché fra loro equivalenti, e come tali universalmente accettate e riconosciute, in quanto emesse in un contesto di regole e procedure uniformate.**

L'Organismo di Certificazione che ha accreditato Agostino Oliveri, opera in conformità a quanto prescritto nei riferimenti **normativi**:

- ✓ UNI CEI EN **ISO/IEC 17024:2004** - Valutazione della Conformità - Requisiti generali per gli organismi operanti la certificazione delle persone.

e nei riferimenti **non normativi**:

- ✓ emessi da ACCREDIA ex SINCERT (es. RT 12, RT 15, ecc…),
- ✓ emessi dall'Ente: Regolamento e Schemi di Certificazione.

L'esperienza maturata da più di venti anni nei vari settori su alcune realtà molto importanti anche multinazionali, fra cui le seguenti, si ritiene rappresenti una garanzia per la realizzazione di un significativo percorso per la Vostra realtà:

- Coopservice (www.coopservice.it)
- Comune di Firenze (www.comenu.fi.it)
- White Rabbit (www.whiterabbit.cloud)
- Toshiba Medical Systems Now Canon Medical Systems (https://eu.medical.canon/italy/)
- Register.it – DADA Group (www.register.it)
- Siena Parcheggi (www.sienaparcheggi.it)
- GlobalPesca (www.globalpesca.it)
- Neotron (www.neotron.it)
- LIBRO CO. ITALIA (www.libroco.it)
- DIGISOFT Group (www.digisoft.it)
- Ermanno Scervino (www.ermannoscervino.com)
- Savino del Bene (www.savinodelbene.com)
- ALHA Group (www.alhagroup.com)
- G.V.M. (www.gvmnet.it)
- Sinergia (www.sinergia.bcC.it)
- Coopersytem (www.coopersystem.bcc.it)
- Terranova (www.terranovasoftware.eu)
- HAVI Logistics (www.havi.com) and Sti-Italy
- Mechanical Diagnosis Mecoli (www.mecoil.net)
- Revet (www.revet.com)
- Opera Diocesana Assistenza (www.odafirenze.it)
- Fratellanza Militare Onlus Firenze (www.fratellanzamilitare.com)
- Caf UGL (www.cafugl.it)
- Ugl (www.ugl.it)
- Laborfonds (www.laborfonds.it)
- Webdev (www.webdev.it)
- Cassa Mutua Toscana (www.mutuabcc.it)
- Gruppo GPI (www.gpi.it)
- Co.Ta.Fi (taxi 4390) (www.4390.it)
- Hal Allergy (www.hal-allergy.com)
- So.Se.Pharm (www.sosepharm.it)
- Special product line (www.specialspa.it)
- Bowe Systec (www.bowe-systec.com)
- Idee per Viaggiare (www.ideeperviaggiare.it)
- Sanifonds (www.sanifonds.tn.it)
- Archimede (www.archimedespa.it)
- LCI Italy Srl (www.lippertcomponents.com)
- Mef (www.mefsrl.it)
- Sixtus Italia (www.sixtusitalia.it)
- Onebroker Srl e Onebroker Veneto Srl

SICURDATA Srl è disponibile a fornire, a integrazione della presente, le evidenze di quanto esposto.

2. SINTESI DELLA PROPOSTA

Con la presente vi indichiamo le caratteristiche tecniche ed economiche del servizio di individuazione e nomina della Figura del Responsabile della Protezione dei Dati (DPO/RPD) per la vostra realtà.

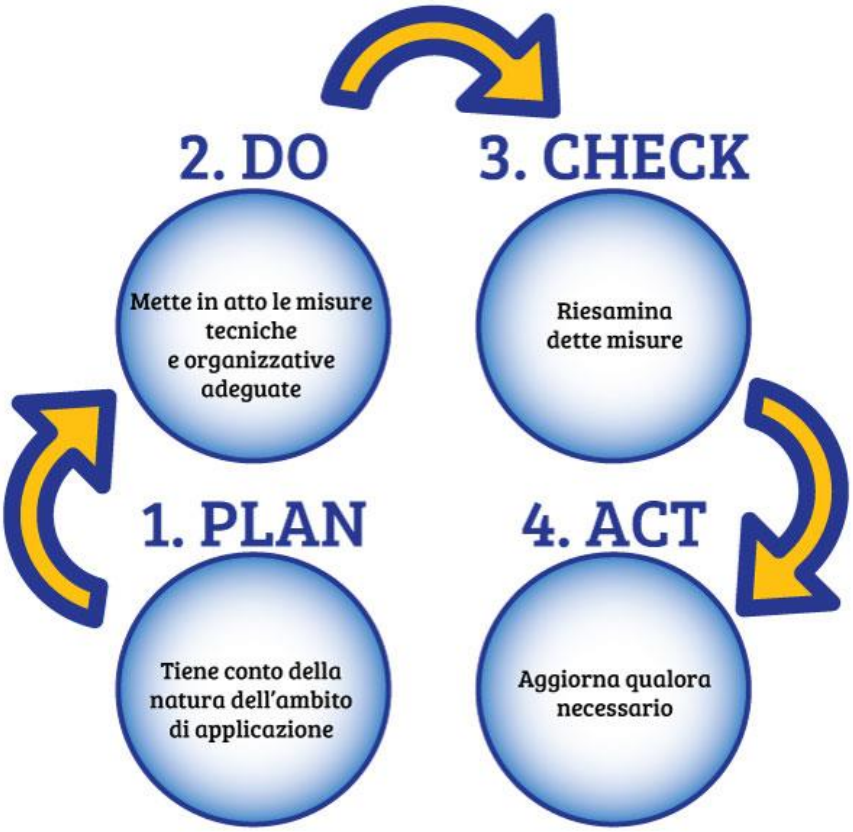
Si chiede e suggerisce per una migliore interpretazione del principio di accountability (responsabilità verificabile) del GDPR :

- La costituzione ufficiale di un G.D.L (Gruppo di Lavoro Privacy) al fine di ottimizzare e recepire al meglio le nostre indicazioni operative e di implementazione del nuovo Sistema di Gestione Privacy. Lo stesso G.D.L. sarà poi individuato e richiamato nelle varie procedure al fine di analizzare preventivamente e tempestivamente ogni eventuale situazione "privacy" tipo le c.d. data breach;

- L'individuazione e ufficializzazione della figura del delegato privacy che possa essere per noi il punto di riferimento e figura centrale del progetto di adeguamento da far crescere al Vostro interno su questa tematica con la supervisione/supporto nostro e la garanzia della validazione da parte del nostro team di consulenza.

Nel caso di accettazione del nostro progetto, sarà fornito e condiviso con il Vostro team:

- GANTT – Piano di lavoro dettagliato e operativo con i vari task e attività da pianificare e relativa scadenza. Si prevede un tempo massimo di 20 giorni per la conclusione del progetto dal momento in cui sia stata svolta la fase 1, salvo diverse comunicazioni. Sarete sempre informati dello stato dell'arte e sarà nostra cura fornire report e mail con stati di avanzamento dei lavori alla Direzione. All'interno di questo piano sarà previsto anche un affiancamento per la verifica di implementazione del nuovo sistema di gestione privacy utilizzando il metodo: Plan - Do - Check – Act :



3. COSTI

C.C.P. di Sicurdata Srl s'impegna e offre i seguenti servizi:

3.1 NOMINA DATA PROTECTION OFFICER

Descrizione	Costo	Timbro e firma per accettazione
Eventuale incarico e nomina di una figura scelta dal C.C.D.P. (Centro Competenza Data Protection & Privacy) di Sicurdata Srl quale DPO/RPD. Il DPO è un supervisor indipendente nella versione inglese si parla infatti del verbo "to monitor" per indicare alcuni dei principali compiti dello stesso dovendo verificare secondo un principio di accountability, che vi sia non solo la consapevolezza dei rischi connessi al trattamento dei dati ma soprattutto che il titolare sia in grado di documentare i controlli effettuati. Il DPO potrà anche essere interno all'azienda oppure esterno in forza di un contratto di servizi, in quest'ultimo caso con una durata minimo di quattro anni. Peraltro, verso, un aspetto troppo spesso trascurato nell'attuale dibattito è che la designazione del DPO è già prevista come obbligatoria da oltre dieci anni nelle istituzioni dell'Unione Europea (regolamento 45/2001). Analogamente, da alcuni anni in diversi Stati Membri - in base all'art. 18 della Direttiva 95/46/Ce - il DPO è obbligatorio (Germania, Grecia, Ungheria, Slovacchia), in altri come in Francia, è invece previsto un DPO ma come una figura facoltativa. Alcuni dei complessi compiti affidati al DPO che si possono elencare sono : 1) sorvegliare sulla corretta applicazione della normativa sulla protezione dei dati europeo ed italiana, nonché l'osservanza del politiche interne, anche compiendo attività di verifica, azioni formative ed informative; 2) fornire pareri e sorvegliare alla corretta esecuzione di una Data protection impact analysis (c.d. Dpia); 3) fungere da contact point e collaborare con l'Autorità Garante per la protezione dei dati personali anche nell'ambito delle verifiche preliminari. L'attività di nomina della figura del Data Protection Officer o Responsabile della Protezione dei dati personali viene garantita individuando una figura con comprovate capacità ed esperienze certificate nel tema della sicurezza nel trattamento dei dati personali. Se la figura è interna non dovrà però avere conflitti di interesse. Nell'eseguire i propri compiti la nuova figura considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.	Alla luce di quanto detto, ad oggi (S.E.& O.) l'attribuzione del ruolo e relativa nomina viene quantificata in **Euro 5.000,00 (cinquemila/00) + IVA anno/DPO** (oltre eventuale rimborso spese di trasferta a piè di lista) con contratto biennale **Sono comprese nel compenso n.3 giornate per le attività di relazioni quadrimestrali.** Nel caso si dovessero pianificare ulteriori interventi come DPO, si dovranno preventivamente e congiuntamente definire i costi e modalità Resta inteso che durante l'anno la presente attività potrà essere rivista e rimodellata secondo i nuovi orientamenti e pronunciamenti dello stesso Garante della Privacy che detterà ulteriori nuove linee guida interpretative.	**Data, Timbro e firma**

3.2 FORMAZIONE SECONDO GDPR 679/2016

Descrizione	Costo	Timbro e firma per accettazione
Soluzione A: Formazione e Addestramento BASE in modalità "FAD" (E-Learning) utilizzando la nostra piattaforma con test finale e rilascio di un attestato di frequenza ad ogni partecipante e al Titolare evidenza e certificazione dell'avvenuta formazione.	**Euro 25,00 (venticinque/00) + IVA** per corso Privacy "BASE" o AVANZATO (Costo una-tantum per ogni utente. Utenti da abilitare preventivamente e congiuntamente)	**Data, Timbro e firma** **Indicare numero utenti**
Soluzione B: Formazione e Addestramento in aula (per un massimo di 15/20 figure per aula) suddividendo le sessioni in funzione del ruolo: incaricati, responsabili e amministratori di sistema. Verrà compilato un registro di presenza/frequenza da mettere agli atti all'interno del proprio DOSSIER PRIVACY e SGP (Sistema di Gestione Privacy) ed ogni partecipante riceverà oltre al materiale didattico anche un attestato personalizzato di partecipazione. Il Cliente si impegna a mettere a disposizione un'aula attrezzata nel rispetto delle attuali norme per il contenimento del Covid19.	**Euro 500,00 (cinquecento/00) + IVA** per ogni aula per una sessione di 3 ore (oltre ad eventuali rimborsi spese di trasferta da calcolare a piè di lista) (Costo una-tantum) (Date da definire preventivamente e congiuntamente)	**Data, Timbro e firma** **Indicare numero aule**

3.3 SUPPORTO SGP COME PREVISTO DAL GDPR 679/2016

Descrizione	Costo	Timbro e firma per accettazione
Attività di straordinaria manutenzione e assistenza come ad esempio: • Aggiornamento DPIA secondo le linee guida ENISA; • Valutazione impatto Decreto sicurezza ed eventuale implementazione; • Valutazione impatto nuove linee guida europee per la politica di conservazione dei dati ed eventuali implementazioni; • Valutazione impatto eventuale entrata in vigore Nuovo Regolamento E-Privacy; • Servizio di "simulazione visita ispettiva"; • Valutazione implementazione servizio di Penetration Test & Vulnerability Assessment ai fini del perimetro di Cybersecurity conforme al principio di Accountability del GDPR; • Rivisitazione policy del sito e policy cookies law, anche alla luce della sentenza corte di giustizia dell' Unione Europea sull'utilizzo dei cookies; • Adeguamento e/o introduzione sistemi di videosorveglianza e/o GPS; • Eventuali richieste da parte degli interessati. **Ogni singola attività verrà erogata solo previa effettiva necessità e specifica richiesta da parte del Cliente.** Le ore saranno preventivamente e congiuntamente concordate. Le ore possono essere utilizzate senza vincolo di ripartizione come sopra esposto e a consuntivo sia in modalità ON SITE sia in modalità IN HOUSE. Mensilmente verranno rendicontate e addebitate le ore effettivamente svolte o frazione di esse.	**Euro 62,00 (sessantadue/00) + IVA** per ogni ora/uomo (oltre eventuale rimborso spese di trasferta a piè di lista).	**Data, Timbro e firma**

4. RIEPILOGO COSTI

I costi sono così riassunti:

- **Nomina DPO**: € 5.000,00 + iva annui (oltre ad eventuali rimborsi spese di trasferta da calcolare a piè di lista)
- **Formazione**: Euro 25,00 + Iva per ogni utente
  e/o Euro 500,00 + Iva per ogni sessione in aula (oltre ad eventuali rimborsi spese di trasferta da calcolare a piè di lista)
- **Supporto S.G.P**.: Proposta contratto a chiamata € 62,00 + IVA per ogni ora/uomo (oltre ad eventuali rimborsi spese di trasferta da calcolare a piè di lista). Ogni ora sarà preventivamente e congiuntamente concordata e solo previa vostra autorizzazione.

5. CONDIZIONI DI FORNITURA

- Il pagamento dovrà avvenire al ricevimento delle singole fatture tramite bonifico bancario;
- Ciascuna parte avrà facoltà di recedere dal Contratto in qualsiasi momento dandone comunicazione scritta all'altra Parte mediante lettera Raccomandata con avviso di ricevimento o PEC, con un preavviso non inferiore a 90 gg.
- Nel caso la nostra offerta fosse di Vostro gradimento è necessario restituire lettera di assegnazione incarico facendo riferimento al numero di progetto riportato in prima pagina firmata per accettazione via mail PEC all'indirizzo sicurdatasrl@pec.opendata-pec.com oppure all'indirizzo privacy@opendata.it.

6. SICURDATA S.R.L. DICHIARA

- di mantenere, per se e per il proprio personale, per tutta la durata della trattativa e successivamente la massima riservatezza circa i fatti, le informazioni, i documenti relativi alla organizzazione, l'attività ed ai piani della Società, le strategie commerciali, piani di investimento, costi, prezzi e profitti, informazioni e dati relativi ai clienti ed ai fornitori, di cui è venuto a conoscenza e di cui verrà a conoscenza in ragione o in occasione dell'esecuzione del Contratto e/o dei Servizi oggetto del presente progetto;
- i dati personali, i dati e le informazioni di natura commerciale, organizzativa, societaria, strategica, ivi comprese chiavi di accesso, password et similia, nonché ogni informazione relativa ai Clienti di cui la Società o il personale verranno a conoscenza in funzione, in esecuzione e comunque in occasione del presente Contratto saranno comunicati e trattati, con la specifica ed esclusiva finalità di adempiere agli obblighi derivanti dall'eventuale incarico e dalla legge;
- che l'aliquota IVA sarà applicata nei termini di legge;
- che tutti i prezzi sono omnicomprensivi dei costi per la sicurezza e di trasferta;
- che nei costi sono compresi i costi di interfacciamento con gli altri professionisti interessati dal processo di adeguamento;
- che l'offerta rimane valida fino all'aggiudicazione della procedura, comunque non oltre 60 giorni dalla ricezione della presente;
- Le attività saranno svolte parzialmente, a seconda delle necessità, presso la sede del cliente.
- Il personale coinvolto nell'erogazione di quanto previsto da questo contratto si impegna a mantenere riservata ogni informazione relativa al cliente di cui dovesse venire a conoscenza e a non praticare azioni di concorrenza sleale o distrazione di personale;
- che per tutto quanto non esplicitamente dettagliato nell'offerta economica, saremo ben lieti di riformulare a fronte di Vostre esplicite richieste il nostro migliore progetto tecnico-Economico;

7. TRATTAMENTO DATI PERSONALI

- Con la sottoscrizione del contratto entrambe le parti si impegnano, ai sensi e per gli effetti di quanto previsto dal Regolamento UE 2016/679 – di seguito anche GDPR - a fare si che tutti i dati personali forniti con il presente contratto saranno utilizzati per le finalità gestionali ed amministrative inerenti all'adempimento degli obblighi contrattuali e legislativi, salvo ulteriori specificazioni previste da ciascuna parte del contratto.
- In caso di sottoscrizione da parte del Cliente, per la fornitura dei Servizi di cui al presente contratto, Sicurdata Srl tratterà i dati personali del Cliente secondo quanto disposto dal Regolamento UE 2016/679. Il trattamento sarà effettuato secondo quanto descritto nell'informativa redatta ai sensi dell'art. 13 GDPR e allegata al presente contratto. Pertanto, prima di fornire qualsiasi dato personale e di firmare il presente contratto, siete pregati di leggere con attenzione tale informativa (all.1). **Si prega di restituire copia firmata dell'allegato n.1**
- Il servizio affidato a Sicurdata S.r.l. può comportare il trattamento di dati personali per conto del Cliente. Ai sensi dell'art. 28 Regolamento UE 2016/679 relativo alla protezione dei dati personali il Titolare del trattamento si può avvalere di uno o più Responsabili del trattamento che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del citato Regolamento e garantisca la tutela dei diritti dell'interessato. In ragione dei sopravvenuti aggiornamenti di tale normativa, che ha abrogato la direttiva Madre 95/46/CE in materia di trattamento dei dati personali e alla luce degli aggiornamenti derivanti dal Dlgs. 101/2018 c.d. "schema di armonizzazione" pubblicato in G.U. il 04.09.2018 e entrato in vigore il 19.09.2018, le parti congiuntamente concordano di nominare Sicurdata Srl quale Responsabile del trattamento ai sensi dell'Art.28 GDPR per i dati di cui potenzialmente viene a conoscenza e che tratta per le attività consulenziali offerte (all.2). **Si prega di restituire copia firmata dell'allegato n.2**

Scandicci, 12/11/2021

Firma

Agostino Oliveri