**Offerta per trattativa diretta n. 681283**

Trattativa diretta (/opencms/opencms/help/pa/Ordini/La_trattativa_diretta/visualizzazione_offerta/Visualizzazione_offerta.html?popup=true)
con un unico operatore economico.

| | |
|---|---|
| **Amministrazione titolare del procedimento** | CONSIGLIO NAZIONALE GEOMETRI E GEOMETRI LAUREATI<br>P.IVA: 80053430585<br>Indirizzo: Piazza Colonna 361 |
| **Punto Ordinante** | PAOLA LAUDATI<br>Telefono: 064203161<br>Fax: 0648912336 |
| **Soggetto stipulante** | PAOLA LAUDATI - CONSIGLIO NAZIONALE GEOMETRI E GEOMETRI LAUREATI |
| **Descrizione richiesta** | SERVIZI DI ADEGUAMENTO AL GDPR |
| **Tipologia di trattativa** | Affidamento diretto (art. 36, c. 2, lett. A, D.Lgs. 50/2016) |
| **Modalità di definizione dell'offerta** | Prezzo a corpo |
| **Termini di pagamento** | 60 GG Data Ricevimento Fattura |
| **CIG** | |
| **CUP** | |
| **IPA - Codice univoco ufficio per Fatturazione Elettronica** | UFM1NI |
| **Dati di consegna** | P.ZZA COLONNA 361 ROMA - 00187 (RM) LAZIO |
| **Dati e aliquote di fatturazione** | Aliquota IVA di fatturazione: 22% Indirizzo di fatturazione: P.ZZA COLONNA 361 ROMA - 00187 (RM) LAZIO |
| **Termine di presentazione dell'offerta** | 22/11/2018 18:00 |
| **Limite di validità dell'offerta** | 07/12/2018 18:00 |
| **Ulteriori note** | |
| **Fornitore** | AVVERA |

Allegati alla richiesta

| Descrizione | Nome file | File |
|---|---|---|
| RICHIESTA DI OFFERTA TECNICA ED ECONOMICA | TRATTATIVA DIRETTA PRIVACY 2018 .pdf | (/tratdirette/manageDocumenti.do?method=downloadDocumentoAllegato&idTrattativa=681283&idAllegato=859662) |

Schede di offerta

| Descrizione | Quantità | Visualizza |
|---|---|---|
| Servizi di supporto specialistico (Scheda di RdO per fornitura a corpo) | 1 | (/tratdirette/manageOffertaSchedaTecnica.do?method=consultaAttributiSchedaTecnica&offertaTrattativa.idOfferta=383030&idTrattativaScheda=1026318&offertaTrattativa.trattativa.idTrattativa=6812 |

| | |
|---|---|
| **Importo da ribassare (Euro)** | 11000 |
| **Prezzo a corpo (Euro)** | 10500,00 |
| **Costi di sicurezza aziendali concernenti l'adempimento delle disposizioni in tema di salute e sicurezza sui luoghi di lavoro, di cui all'art. 95, comma 10, del D. Lgs. n. 50/2016** | 400,00 |
| **Data di presentazione dell'offerta** | 21/11/2018 08:29 |

Offerta economica

| Nome documento | Scarica documento | Esito verifica firma |
|---|---|---|
| TD681283_Offerta_AVVERA__ID383030.pdf.p7m | (/tratdirette/manageDocumenti.do?method=downloadDocumentoOffertaFirmato&idOfferta=383030) | |

Documenti richiesti (oltre all'offerta)

| Nome documento | Firmato | Scarica documento | Esito verifica |
|---|---|---|---|

Documento pubblicato sul sito del CNGeGL, Sezione Amministrazione trasparente! 14/12/18

[redacted] Nome documento (http://www.consip.it/) Firma Ministero dell'Economia e delle Finanze (http://www.mef.gov.it/) Scarica documento verifica firma

ULTERIORI DOCUMENTI RITENUTI UTILI SI (/tratdirette/manageDocumenti.do?method=downloadDocumentoAggiuntivo&idRichiesta=462206)

INDIETRO | INVIA PER LA STIPULA | RIFIUTA

## Contatti

*dal lunedì al venerdì dalle 9.00 alle 18.00*

PA **{{numeroVerdePA}}**
(numero verde unico)

IMPRESE **{{numeroVerdeIM}}**
(per malfunzionamenti sul Portale Acquisti in Rete)

Vedi tutti i contatti

## Seguici su

YouTube (https://www.youtube.com/channel/UC426bjPolvTwyVPiTHyyhEg)

Twitter (https://twitter.com/Consip_Spa?ref_src=twsrc%5Etfw)

Telegram (https://t.me/ConsipSpa)

Instagram (https://www.instagram.com/consipspa/)

Link Veloci

Vetrina Iniziative (/opencms/opencms/vetrina_inizlative.html)

Vai al Catalogo (/opencms/opencms/categoriaProdotti.html)

Supporto

Come Iniziare

Filmati Dimostrativi (/opencms/opencms/filmati.html)

Domande Frequenti (/opencms/opencms/faq.html)

Accessibilità (/opencms/opencms/accessibilita.html)

Vetrina Bandi (/opencms/opencms/vetrina_bandi.html)

Obbligo – facoltà (/opencms/opencms/programma_comeFunziona_obblighi_facolta.html)

Guide Operative (/opencms/opencms/supporto_guide.html)

Eventi e Formazione (/opencms/opencms/supporto_Eventi-Formazione.html)

Portale

Manutenzione (/opencms/opencms/manutenzione.html)

Note Legali (/opencms/opencms/note_legali/responsabilita.html)

A V V E R A

*ATTIVITÀ CONSULENZIALI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI.*

# 1. INDICE

## 2. PROFILO AZIENDALE

L'introduzione di normative sempre più stringenti in materia di Responsabilità Amministrativa degli Enti, Antiriciclaggio, Privacy e Salute e Sicurezza nei Luoghi di Lavoro ha determinato un'estensione degli obblighi che gravano sulle imprese e un allargamento del perimetro di responsabilità del management.

Anche in considerazione delle sanzioni amministrative e penali notevolmente afflittive, è raccomandabile l'adozione di nuovi modelli organizzativi e di strategie di riduzione dei rischi in grado di salvaguardare il management e il patrimonio economico e reputazionale della società su cui gravano le predette responsabilità ed oneri.

L'ampiezza dei processi, delle funzioni e dei sistemi coinvolti, richiedono un approccio innovativo e maggiormente integrato rispetto a quello della tradizionale consulenza legale.

**Avvera S.r.l.** (di seguito **Avvera**) nasce con la missione di fornire alle aziende un supporto consulenziale e operativo per la gestione dei rischi operativi e legali d'impresa. Il *core business* di Avvera è l'affiancamento del cliente finalizzato allo sviluppo di un efficace sistema di riduzione del rischio con un approccio che riconduca ogni azione di conformità all'interno di una strategia più ampia e integrata di Governance, Risk Management e Compliance.

Nell'ambito delle attività consulenziali in materia di protezione dei dati personali Avvera assiste inoltre i propri clienti nel disbrigo di tutte le pratiche connesse agli adempimenti previsti dalla normativa, compresa la formazione, la gestione dei rapporti con interessati e Autorità Garante, etc...

Avvera è società certificata ISO 9001, ISO 27001 e OHSAS 18001. Per svolgere il servizio oggetto dell'offerta, Avvera metterà a disposizione il proprio team di esperti in tematiche legali e informatiche. Nel team di Avvera sono presenti professionisti certificati da TÜV Italia quali Privacy Officer e Consulente della Privacy.

Avvera intende mettere a disposizione del cliente la propria pluriennale esperienza nelle attività di consulenza sia nel settore privato (per società operanti in ambito bancario, finanziario, assicurativo, editoriale di stampa periodica e quotidiana, sanitario, chimico, edile, civile, farmaceutico) che nel settore pubblico e nel terzo settore.

## 3. PREMESSE

Il Regolamento Generale sulla Protezione dei Dati, noto come GDPR (General Data Protection Regulation), comporta alcuni importanti cambiamenti nell'approccio di titolari del trattamento e responsabili del trattamento alla normativa in materia di protezione dei dati personali. Il GDPR, così come descritto nell'ambito del considerando 11, introduce nuovi diritti in capo agli interessati, specifici doveri in capo a coloro che effettuano e determinano il trattamento dei dati personali e modifica il modo di rapportarsi con il Garante per la protezione dei dati personali, prevedendo istituti quali la notifica di violazione, la figura del Responsabile della Protezione dei Dati (noto anche come DPO) ed i principi del "*one stop shop*", "privacy *by design*", "privacy *by default*".

Ai sensi dell'articolo 83 del GDPR il titolare e/o il responsabile possono incorrere in sanzioni amministrative fino a 20 milioni di euro o al 4 % del fatturato globale. Il GDPR (articolo 82) prevede la possibilità per l'interessato di richiedere un risarcimento al titolare anche in caso di danni non meramente materiali.

Il GDPR si applica al trattamento dei dati personali effettuato da parte di un titolare del trattamento nell'ambito delle attività di uno stabilimento sito in uno stato dell'UE, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

Il GDPR si applica inoltre al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento; oppure b) il monitoraggio del comportamento di interessati nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Il GDPR non trova applicazione rispetto al trattamento di dati personali effettuato in stabilimenti siti fuori dall'UE e riferito a interessati che si trovano fuori dall'UE.

# 4. PROPOSTA

Oggetto della presente proposta è collaborare con apporto di metodo, strumenti e risorse per conseguire la corretta implementazione di un efficace modello organizzativo in materia di protezione dei dati personali aggiornato rispetto alle disposizioni del Regolamento UE.

Con riferimento ai trattamenti di dati personali effettuati dall'Ente in parola si rileva che ricadono nell'ambito di applicazione del GDPR unicamente i trattamenti effettuati in eventuali uffici dello stesso Ente siti nel territorio dell'UE o i trattamenti effettuati in occasione dell'offerta di prestazione di servizi che riguardano dati personali di interessati che si trovano nell'unione (indifferentemente dallo stabilimento del titolare).

## 4.1 MESSA A NORMA

Avvera, con l'indispensabile collaborazione delle risorse interne del cliente, provvederà a porre in essere una attività di messa norma per l'Ente.

L'intervento di messa a norma comprenderà la predisposizione della documentazione da utilizzarsi secondo le rilevazioni effettuate nella fase di assessment.

L'intervento di messa a norma, ove risulti applicabile il GDPR, comprenderà inoltre:

- la redazione di un registro dei trattamenti,
- la redazione della valutazione dei rischi,
- la redazione della valutazione degli impatti,
- l'analisi dell'esigenza di dotarsi del Responsabile per la protezione dei dati personali.

Tutta la documentazione scaturita dalle suddette attività di messa a norma è di proprietà del Cliente ed è resa gratuitamente ed immediatamente disponibile al Cliente stesso in formato PDF/Word sia in fase di 1^ predisposizione che di aggiornamento.

Avvera consegnerà altresì al Cliente in busta sigillata i dati inerenti le pesature delle contromisure utilizzate in occasione delle attività di analisi del rischio. Tale documento contiene segreti industriali di Avvera e viene consegnato a garanzia per essere utilizzato solamente in uno dei seguenti casi:

- liquidazione di Avvera s.r.l.;

- fallimento o sottoposizione a procedure concorsuali di Avvera S.r.l.,
- controllo da parte dell'autorità Garante per la protezione dei dati personali.

In ogni altro caso, il Cliente dovrà chiedere supporto ad Avvera laddove avesse necessità di ottenere dette informazioni. Il Cliente dovrà custodire e proteggere adeguatamente i dati e il supporto che li contiene.

Di seguito una spiegazione della attività comprese nelle attività qui sopra richiamate.

### 4.1.1 PREDISPOSIZIONE DELLA DOCUMENTAZIONE DA UTILIZZARSI

Avvera, sulla base delle informazioni fornite e delle necessità individuate, provvederà a fornire la documentazione necessaria affinché la società risulti pienamente conforme al Regolamento (UE) 2016/679.

A titolo esemplificativo Avvera provvederà a mettere a disposizione i seguenti documenti:

- adempimenti di rilevanza interna o prodromica agli adempimenti successivi:
  - *formulazione di un organigramma privacy;*
- adempimenti nei confronti dei dipendenti e collaboratori:
  - *informative e moduli di richiesta dei consensi (nei casi in cui saranno ritenuti necessari),*
  - *individuazione degli incaricati del trattamento e predisposizione della relativa documentazione,*
  - *predisposizione di linee guida, istruzioni, regolamenti per il corretto trattamento dei dati personali;*
- adempimenti nei confronti degli interessati, a titolo esemplificativo:
  - *informative, associati, utenti, fornitori, ecc.,*
  - *informative e consensi per il canale web (navigazione sul sito, richiesta informazioni, acquisti, newsletter, ecc.),*
  - *informative per soggetti ripresi dalle videocamere di sorveglianza;*
  - *ect.*
- adempimenti nei confronti di fornitori e partner per regolamentare i flussi di informazioni scambiati, quali nomina dei responsabili "esterni" del trattamento.

## 4.1.2 REGISTRO DEI TRATTAMENTI

Il GDPR prevede che il titolare del trattamento, per dimostrare che si conforma al Regolamento stesso, debba tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità.

Tale registro deve contenere tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese;

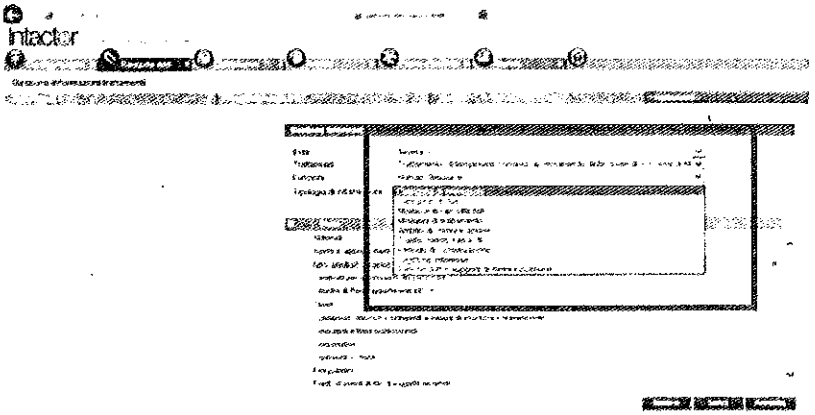
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

Il registro deve essere tenuto in forma scritta, anche in formato elettronico e deve essere messo a disposizione dell'autorità di controllo.

Nell'ambito dell'intervento di cui alla presente offerta sarà predisposto un registro del trattamento.

Avvera effettuerà le attività in parola utilizzando uno strumento informatico proprietario. Lo strumento consente di censire una serie di informazioni per ogni trattamento del cliente.




Per ogni trattamento vengono raccolte le seguenti tipologie di informazioni:

- Categorie di dati
- Categorie di interessati
- Modalità di raccolta dati
- Modalità di trattamento
- Ambito di comunicazioni
- Trasferimento Extra U.E.
- Periodo di conservazione
- Legittimo interesse
- Banche dati e supporti di memorizzazione
- Condizioni DPIA

Le informazioni raccolte nella seguente fase confluiscono nel registro dei trattamenti (Parte I Registro dei trattamenti).

## 4.1.3 VALUTAZIONE DEI RISCHI

Le previsioni del Regolamento in tema di misure di sicurezza integrano il concetto di livello adeguato di sicurezza già proprio della direttiva 95/46/CE. Rispetto a tale concetto di adeguatezza, la necessità di operare in conformità alla normativa in materia di protezione dei dati personali aveva già negli anni evidenziato l'opportunità che i titolari del trattamento procedessero internamente ad una analisi dei rischi incombenti sui dati personali oggetto di trattamento (e non solo rispetto ai trattamenti mediante sistemi informatici). Tale attività di misurazione rientrava inoltre, nell'ambito della applicazione in Italia della normativa in materia di protezione dei dati personali, tra gli elementi che componevano il Documento Programmatico sulla Sicurezza.

Il Regolamento ha, come sopra accennato, integrato il concetto di adeguatezza precedentemente noto, introducendovi due elementi di assoluta rilevanza:

- i costi di attuazione;
- la misurazione di probabilità e gravità dei rischi per i diritti e le libertà delle persone fisiche.

Il concetto di adeguatezza riferito alle misure di sicurezza nell'ambito nel Regolamento necessita quindi di una procedura di analisi e valutazione più articolata rispetto a quella adottabile in adempimento della normativa previgente. La valutazione di adeguatezza delle misure tecniche e organizzative che il titolare del trattamento mette in atto è legata, in ragione della formulazione dell'articolo 32 del Regolamento, con la necessità di definite un livello di sicurezza che il soggetto decisore designa come adeguato rispetto al rischio. Per procedere alla valutazione di adeguatezza delle misure di sicurezza queste andranno valutate in ragione della loro capacità di prevenire e mitigare i rischi che incombono sui dati personali oggetto di trattamento; sarà pertanto necessario:

- valutare i rischi della sicurezza (rischi che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati);
- considerare i costi di attuazione;
- misurare come i rischi possano impattare sul soggetto cui i dati personali si riferiscono.

Avvera ha sviluppato internamente una dettagliata ed approfondita metodologia di analisi dei rischi, avendo riguardo a standard internazionalmente riconosciuti quali gli standard ISO/IEC 27001:2013 Information Technology - Security Techniques - Information Security Management Systems - Requirements e ISO/IEC 27002:2013 - Information Technology - Security techniques - Code of Practice for information security management. La metodologia di Avvera è in grado di supportare concretamente ed efficacemente il cliente nella definizione di un adeguato livello di protezione dei dati personali trattati.

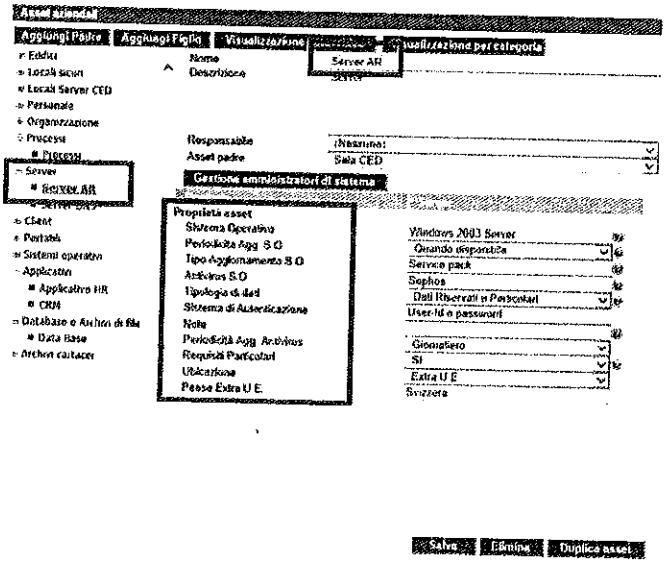
La metodologia prevede l'individuazione degli asset aziendali suddivisi in macro categorie predefinite. In particolare verranno mappati i seguenti asset:

- Edifici
- Locali sicuri
- Locali Server CED
- Personale
- Organizzazione
- Processi
- Server
- Client
- Portatili
- Sistemi operativi
- Applicativi
- Database e Archivi di file
- Archivi cartacei
- Periferiche
- Strumenti di rete
- Strumenti di comunicazione
- Strumenti di sicurezza
- Supporti removibili

Per ogni macro categoria è possibile inserire un numero infinito di assett, ad esempio per la categoria Server:

- Server Contabilità

- Server HR
- Server Posta Elettronica
- Server Documenti aziendali
- Etc.




La metodologia prevede inoltre l'individuazione delle contromisure applicabili ed applicate. Lo status di ogni contromisura può essere:

- [SI] Applicata – per quelle contromisure già implementate;
- [NO] Non Applicata – per quelle contromisure applicabili che non sono state attuate e per le quali non è in corso la fase di implementazione;
- [I/A] In Attuazione – per quelle contromisure che non sono attualmente implementate ma per le quali è già in corso la fase di implementazione ed è stata definite la tempistica di attuazione;
- [N/A] Non Applicabile – per le contromisure che non possono essere applicate per motivi tecnici, logistici o di altra natura;
- [D/F] Da Fare – per quelle contromisure che non sono attualmente implementate ma per le quali si prevede l'implementazione in tempi stabiliti.

In particolare è possibile esaminare 62 gruppi di contromisure:

| | GRUPPI DI CONTROMISURE |
|---|---|
| 01 | Sistemi di Identificazione e Autenticazione |
| 02 | Sistemi di Autorizzazione e Controllo Accessi Logici |
| 03 | Verifiche e Controlli |
| 04 | Riutilizzo di supporti |
| 05 | Vulnerabilità tecniche / Test di sicurezza |
| 06 | Protezione contro il software maligno |
| 07 | Computer portatili, telelavoro e smart-working |
| 08 | Controlli sulle modifiche del software |
| 09 | Controlli sugli Input ed output di sistema |
| 10 | Gestione della sicurezza della rete |
| 11 | Posta elettronica e accesso al web |
| 12 | Autorizzazione clientela |
| 13 | Smartphone e chiavette UMTS |
| 14 | Controllo delle intrusioni |
| 15 | Non ripudio |
| 16 | Confidenzialità dei dati in rete |
| 17 | Controllo accessi alla rete |
| 18 | Reti Wireless e Voip |
| 19 | Sicurezza nel routing |
| 20 | Protezioni fisiche della rete |
| 21 | Sicurezza nell'e-commerce |
| 22 | Cookie e Mobile Code |
| 23 | Capacità del sistema di rete |
| 24 | Controlli antispamming |
| 25 | Qualità dei servizi di rete |
| 26 | Protezioni contro attacchi di denial of service |
| 27 | Controllo sulle operazioni |
| 28 | Controlli Amministrazione di sistema |
| 29 | Controlli sviluppo applicativi |
| 29 | Controlli sviluppo applicativi |
| 30 | Verifica delle attività svolte dai programmatori |
| 31 | Distribuzione e vendita del software |
| 32 | Controlli sulla manutenzione del software |
| 33 | Controlli sulla manutenzione dell'hardware |
| 34 | Controllo errori utenti |
| 35 | Controlli sugli input ed output delle applicazioni |
| 36 | Controlli sui sistemi contabili |
| 37 | Controlli sui supporti di output |
| 38 | Controlli su documenti e supporti |
| 39 | Opzioni di recovery per apparecchiature di rete |
| 40 | Business Continuity Plan |
| 41 | Back-up delle informazioni |
| 42 | Capacity Planning |
| 43 | Protezione da malfunzionamenti di strumenti |
| 43 | Protezione da malfunzionamenti di strumenti |
| 44 | Cloud Computing |
| 45 | Sicurezza fisica edifici |
| 46 | Spostamenti e movimentazioni di beni |
| 47 | Sicurezza fisica dei locali |
| 48 | Protezione contro furti |
| 49 | Protezione beni e strumenti |
| 50 | Terrorismo ed estremismo |
| 51 | Protezione incendi |
| 52 | Protezione allagamenti |
| 53 | Protezione disastri naturali e ambientali |
| 54 | Sicurezza delle risorse energetiche e protezione ambientale |
| 55 | Sicurezza e personale |
| 56 | Sensibilizzazione e formazione in materia di sicurezza |
| 57 | Policy e procedure operative (ISMS) |
| 58 | Infrastrutture di sicurezza (ISMS) |
| 59 | Rapporti con terze parti (outsourcing) e clienti |
| 60 | Gestione incidenti |
| 61 | Verifiche di conformità |
| 62 | Coperture assicurative |

La valutazione dei rischi e la conseguente valutazione di adeguatezza delle misure di sicurezza è quindi articolata nella analisi sistematica dei seguenti fenomeni:

- la reale probabilità che un evento dannoso accada;
- la vulnerabilità dell'oggetto di analisi, rispetto agli eventi minacciosi;
- la magnitudo dell'evento rispetto alla sicurezza di un sistema;
- la magnitudo dell'evento rispetto ai diritti e alle libertà fondamentali dei soggetti a vario titolo interessati;
- la valenza preventiva delle contromisure implementate;
- la valenza mitigativa degli effetti dannosi delle contromisure implementate;
- l'individuazione di una soglia nel rapporto costi benefici delle contromisure implementabili.

In considerazione di quanto sopra, la valutazione del rischio viene effettuata sulla base della seguente formula:

$$R = P \times V \times \left(\frac{100 - CP}{100}\right) \times I \times \left(\frac{100 - CM}{100}\right)$$

dove:

- R = Rischio (in termini di valore);
- P = Probabilità di accadimento (in termini di valore);
- V = Vulnerabilità dell'asset (in termini di valore);
- CP = Capacità Preventiva delle Contromisure (in termini percentuali su una scala compresa tra 0 e 100);
- I = Impatto (in termini di valore);
- CM = Capacità Mitigativa delle Contromisure (in termini percentuali su una scala compresa tra 0 e 100).

Come indicato nella formula precedente, la misurazione e la classificazione dei rischi incombenti sul sistema informativo aziendale e sui dati personali trattati si ottengono rapportando, per ciascun asset analizzato, la probabilità che una minaccia si verifichi con il livello di vulnerabilità dell'asset stesso (correlato alla capacità

preventiva delle contromisure) e il probabile impatto previsto in caso di incidente di security (correlato alla capacità mitigativa delle contromisure).

Le valutazioni sono effettuate mediante metodi misti (qualitativi e quantitativi).

Nell'ambito dell'intervento di cui alla presente offerta sarà predisposto un documento di valutazione dei rischi in cui i risultati sono evidenziati sia in forma tabellare che in forma grafica.

### 4.1.4 VALUTAZIONE DEGLI IMPATTI

La valutazione di impatto sulla protezione dei dati, nota come DPIA, è uno strumento previsto nell'ambito del Regolamento per individuare e analizzare i rischi che incombono sulle persone fisiche. Si tratta di uno degli strumenti che sono stati introdotti in sostituzione degli obblighi generali di notificare alle autorità di controllo il trattamento dei dati personali previsti dalla direttiva 95/46/CE e che nel tempo si sono rivelati inadeguati a migliorare la protezione dei dati personali. La valutazione di impatto è richiesta al fine di individuare appropriate misure rispetto ai rischi che, a seguito della valutazione di adeguatezza, risultino di particolare magnitudo per i diritti e le libertà delle persone fisiche. Ai sensi dell'articolo 35 del Regolamento la valutazione di impatto è prescritta (successivamente alla entrata in vigore del regolamento, quindi per i trattamenti attivati successivamente al 25 maggio 2018) per quei trattamenti, o insiemi di trattamenti, che presentano rischi elevati per gli interessati e tra questi sono espressamente indicati i trattamenti:

a) che comportano una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) che, su larga scala, hanno ad oggetto categorie particolari di dati personali o di dati relativi a condanne penali e a reati; o

c) configurabili quali sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La valutazione di impatto è inoltre obbligatoria rispetto ad un elenco puntuale di trattamenti che il Garante nazionale dovrà rendere noto, con proprio atto, entro il 25 maggio 2018.

L'articolo 35 del Regolamento definisce, nella sua formulazione, uno standard minimo sulla base del quale articolare la valutazione di impatto. Il punto di partenza dell'analisi è individuato nella redazione di una descrizione sistematica dei trattamenti che presentano i rischi elevati e delle finalità perseguite. Sulla base della descrizione il titolare è quindi chiamato ad effettuare una valutazione:

- della necessità e proporzionalità dei trattamenti in relazione alle finalità perseguite,
- oltre che dei rischi per i diritti e le libertà degli interessati.

Il Regolamento dispone che in essa siano descritte le misure con cui il titolare del trattamento prevede di affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento stesso. Tali misure debbono tenere conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione. Va sottolineato che il Regolamento non ha definito alcuna specifica istruzione in merito all'output della valutazione, ma ha previsto che l'Autorità Garante debba essere consultata qualora si evidenzi un rischio elevato in assenza di misure atte ad attenuare il rischio. In merito al rischio elevato che porta alla necessità di consultazione preventiva del Garante, il considerando 84 del Regolamento chiarisce che esso è individuabile nei casi in cui il titolare non possa attenuarlo mediante misure opportune in termini di tecnologia disponibile e costi di attuazione.

La metodologia per la valutazione di impatto sulla protezione dei dati utilizzata da Avvera è schematizzabile in tre momenti.

Nel primo momento sono attivate le iniziative preliminari allo svolgimento della valutazione di impatto. Rientrano in tale fase:

- la definizione in merito alla necessità di effettuare la valutazione di impatto;
- la progettazione della valutazione di impatto, con ciò intendendo l'identificazione dell'oggetto, degli attori, degli stakeholder, dei requisiti normativi;
- l'individuazione della sussistenza di vincoli normativi ulteriori e differenti rispetto a quanto disposto dal Regolamento (a titolo esemplificativo, norme di settore, regolamenti di authority e soggetti regolatori, ecc.).

Il primo momento è chiuso con una chiara individuazione dell'oggetto della valutazione di impatto rispetto al quale le successive fasi devono poi restituire un preciso riscontro.

Il secondo momento prevede interventi finalizzati all'individuazione delle modalità idonee a prevenire il verificarsi dei rischi per i diritti e le libertà fondamentali dell'interessato. Sono eseguiti nell'ambito di tale momento:

- l'individuazione di obiettivi precisi in termini non solo di sicurezza, ma in generale di conformità al GDPR;
- l'individuazione di fonti di rischio;
- una valutazione ponderata della efficacia delle misure adottate e da adottarsi.

Devono essere parte della fase di valutazione le considerazioni formulate dal titolare relativamente a sorgenti di rischio, motivazioni e obiettivi di comportamenti ostili; in questa parte della valutazione hanno sicuramente rilevanza primaria le considerazioni formulate nell'ambito della valutazione di adeguatezza delle misure di sicurezza.

Nella effettuazione delle valutazioni di impatto vi è il confronto tra le misure di sicurezza adottate e standard di sicurezza definiti a priori.

Trova applicazione, nella attività di cui al presente capitolo, il principio per il quale non è consentito un approccio rispetto ai rischi che incombono sugli interessati che si limiti a porre in essere il minimo necessario. È stato infatti già riferito in precedenza come la presenza di un livello di accettazione del rischio non è recepibile in questo specifico iter valutativo. È comunque ipotizzabile, in linea con le previsioni dello stesso Regolamento, dare priorità a quelle soluzioni che assicurano il beneficio più elevato.

Nel terzo e ultimo momento dell'iter di valutazione dell'impatto ha rilevanza fondamentale la reportistica.

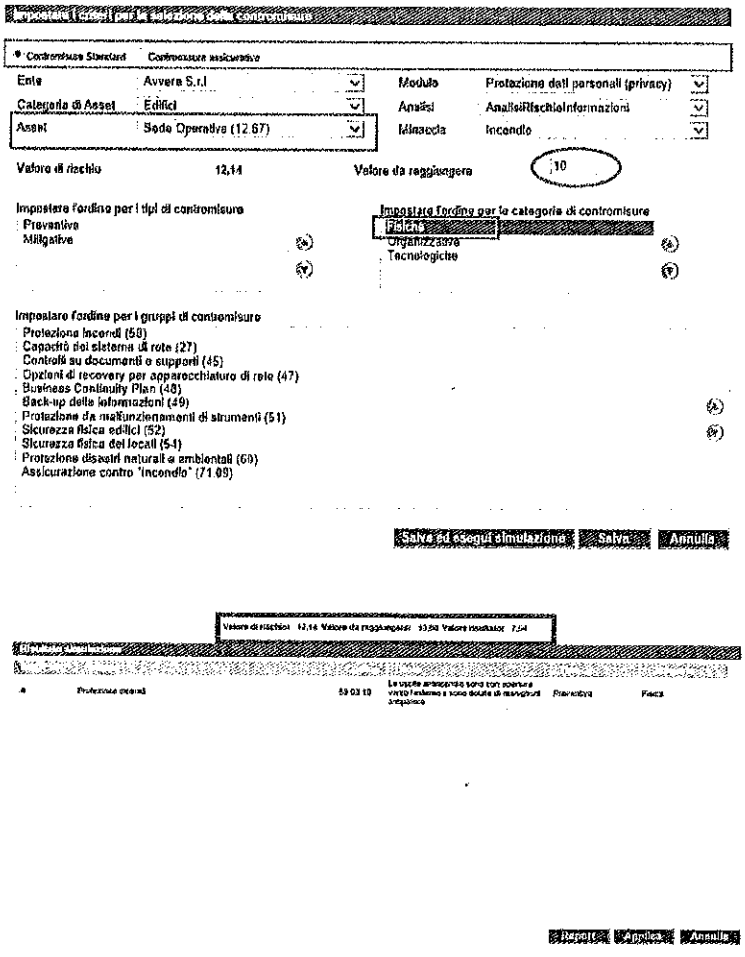
Nell'ottica del principio dell'accountability Avvera fornirà consulenza al cliente perché predisponga documentazione adeguata ad evidenziare le valutazioni poste in essere e le conseguenti soluzioni che sono o devono essere adottate.

Avvera effettuerà le attività in parola utilizzando uno strumento informatico proprietario. Tale strumento consente la raccolta ed esposizione degli elementi di conformità esposti anche nell'ambito dei precedenti passaggi metodologici secondo le indicazioni formulate dal WP29 (Articolo 29 - Data Protection Working Party) nel documento Guidelines on Data Protection Impact Assessment (DPIA).

Lo strumento informatico proposto da Avvera consente di predisporre il cosiddetto "*piano di trattamento del rischio*".

Qualora infatti i risultati delle valutazioni di impatto facciano emergere, rispetto alle soglie prestabilite, un rischio non accettabile per i diritti e le libertà delle persone fisiche il Titolare del trattamento dovrà individuare le misure organizzative e tecniche necessarie per far rientrare il valore del rischio in una soglia accettabile.

Il Titolare potrà valutare le misure da applicare a ciascun asset ai fini di ridurre il rischio fino a una soglia stabilita scegliendo tra la tipologia di misure (fisiche, organizzative e tecnologiche). Attraverso la simulazione potranno quindi essere individuate le misure necessarie a protezione dei dati e potranno essere pianificati gli interventi necessari per una completa compliance.



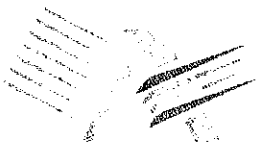

Nell'ambito dell'intervento di cui alla presente offerta sarà predisposto un documento di valutazione di impatto e il relativo piano di trattamento del rischio che le funzioni preposte dovranno poi validare.

La valutazione degli impatti sarà svolta nei casi prescritti dal Regolamento o da provvedimenti dell'autorità Garante.

## 4.1.5 ACCETTAZIONE DEL RISCHIO

Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito il "Regolamento") prevede diversi adempimenti di natura tecnica ed organizzativa al fine di garantire l'adozione di un adeguato livello di protezione per i dati personali trattati.

In merito l'articolo 32, comma 1, del Regolamento prevede che: "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 titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio". Nel valutare l'adeguato livello di sicurezza, si terrà conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. Il comma 3 del citato articolo 32 del Regolamento dispone che l'adesione a un codice di condotta approvato, di cui all'articolo 40 del medesimo Regolamento, o a un meccanismo di certificazione approvato di cui all'articolo 42 dello stesso Regolamento, può essere utilizzata come elemento per dimostrare la conformità ai requisiti di adeguatezza di cui al primo comma del citato articolo 32 del Regolamento.



In mancanza di codici di condotta e standard formalmente e ufficialmente riconosciuti, ai sensi e per gli effetti di cui ai citati articoli 32, 40 e 42 del Regolamento, la valutazione di adeguatezza può essere effettuata alla luce dei seguenti parametri di riferimento:

a. **Misure Minime di sicurezza ICT per le Pubbliche Amministrazioni** (parte integrante delle "*Linee guida per la sicurezza ICT delle Pubbliche Amministrazioni*"), di cui alla Direttiva del Presidente del Consiglio dei

Ministri del 1agosto 2015, ver. 1.0. del 26 aprile 2016 (Agenzia per l'Italia Digitale).

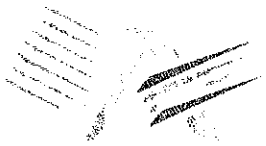
Relativamente al punto b. in fase di analisi si andrà a verificare le Misure presenti. Tali misure sono suddivise in Minime (M), Standard (S), Alte (A).

## 4.1.6 ANALISI ESIGENZA DPO

Avvera procederà ad effettuare un'analisi del modello organizzativo, alla luce del Regolamento (Articoli 37, 38 e 39 GDPR) e delle linee guida "*Guidelines on Data Protection Officers ('DPOs')*" pubblicate dal Gruppo Articolo 29, ai fini di formalizzare un documento comprovante le scelte del Titolare in merito all'individuazione del Responsabile per la protezione dei dati personali o DPO).

La documentazione che Avvera predisporrà nell'ambito della presente attività sarà corredata da (se necessario):

- documento di nomina al DPO;
- documento descrittivo delle istruzioni e dei poteri al DPO;
- documento descrittivo della procedura per la gestione dei processi privacy inerenti al DPO.



## 4.1.7 DELIVERABLE

L'intervento di messa a norma avrà quale deliverable i seguenti documenti:

- documenti di cui al punto 4.1.1;
- registro dei trattamenti di cui al punto 4.1.2;
- valutazione dei rischi di cui al punto 4.1.3;
- valutazione degli impatti di cui al punto 4.1.4 (se necessaria, per i trattamenti attivati successivamente al 25 maggio 2018);
- Analisi esigenza DPO di cui al punto 4.1.6..

# 5. ASSUNZIONI

Al fine di garantire la qualità dei servizi di consulenza devono essere rispettate le assunzioni riportate di seguito:

- Il Cliente fornirà tutta la documentazione necessaria per consentire la conoscenza delle informazioni indispensabili al fine di svolgere correttamente le attività progettuali in ambito alla presente Proposta;
- Relativamente al capitolo 4.1, si assume che la raccolta delle informazioni avvenga mediante interviste on site per un massimo di tre 3 gg;
- Il Cliente garantirà il supporto relativamente a:
  - interfacciamento con i referenti di applicazioni e/o sistemi al fine di reperire informazioni utili alle attività in ambito alla presente offerta,
  - interpretazione degli standard tecnici, procedurali ed organizzativi,
- Il Cliente garantirà la disponibilità e l'effettivo coinvolgimento delle sue risorse interne e degli eventuali propri fornitori/Terze Parti, nonché la produzione da parte di essi dei risultati di progetto di competenza secondo i tempi e i modi concordati (l'efficacia di questo coinvolgimento costituisce condizione necessaria per la corretta esecuzione della prestazione).

# 6. PROFILI CONSULENZIALI

Per la realizzazione delle attività verranno impiegati i seguenti profili consulenziali:

**Legal Consultant** - Consulente legale, certificato TÜV Italia "Privacy Officer e Consulente della Privacy", con pluriennale esperienza in normativa in materia di protezione dei dati personali e data protection.

**Legal Consultant Junior** - Consulente legale, con esperienza in normativa in materia di protezione dei dati personali e data protection.

## 6.1 LEGAL CONSULTANT

| **Profilo** | **Consultant con esperienza pluriennale in materia di Data Protection e Risk Assessment** | |
|---|---|---|
| **Functional/Industry Expertise** | **Functional Experience**<br>▪ Data Protection<br>▪ Risk Assessment<br>▪ Audit<br>▪ Certificazione delle Competenze come "Privacy Officer e Consulente della Privacy" secondo lo Schema CDP | **Industry Experience**<br>▪ Fashion<br>▪ Luxury brands<br>▪ Financial Services<br>▪ Chemical<br>▪ Healthcare<br>▪ Pharmaceutical<br>▪ Pubblic authority |
| **Esperienze selezionate** | ▪ **Consulente ISO/IEC 27001:2013:**<br>• Attività di consulenza e supporto allo sviluppo del Sistema di Gestione della Sicurezza delle Informazioni secondo lo standard ISO/IEC 27001:2013<br><br>▪ **Privacy Consultant:** consulenza in materia di data protection nei seguenti ambiti:<br>• Attività di audit e risk assessment;<br>• Elaborazione di modelli organizzativi privacy;<br>• Attività di redazione documentale e revisione dei contratti;<br>• Verifica del rispetto delle misure minime di sicurezza (Allegato B, D. Lgs. 196/2003);<br>• Supporto allo sviluppo di nuovi progetti secondo un approccio Privacy by Design | |

## 6.1 LEGAL CONSULTANT JUNIOR

| | | |
|---|---|---|
| **Profilo** | **Consultant con esperienza in materia di Data Protection e Risk Assessment** | |
| **Functional/Industry Expertise** | **Functional Experience**<br>▪ Data Protection<br>▪ Risk Assessment<br>▪ Audit | **Industry Experience**<br>▪ Financial Services<br>▪ Marketing |
| **Esperienze selezionate** | ▪ **Privacy Consultant:** consulenza in materia di data protection nei seguenti ambiti:<br>• Attività di audit e risk assessment;<br>• Elaborazione di modelli organizzativi privacy;<br>• Attività di redazione documentale;<br>• Verifica del rispetto delle misure minime di sicurezza (Allegato B, D. Lgs. 196/2003). | |

# 7. TEMPISTICHE DI INTERVENTO

Qui di seguito riportiamo un'ipotesi di scadenze per le attività previste nel presente documento.

In caso di accettazione della presente offerta entro il 10 dicembre 2018.

**Entro il 31 dicembre 2018:**

- Analisi siti Internet;
- Predisposizione di informative e consensi di cui al punto 4.1.1;
- Analisi esigenza DPO di cui al punto 4.1.6 e predisposizione modello di nomina;

**Entro gennaio 2019:**

- Predisposizione della documentazione idonea a distribuire compiti e responsabilità di cui al punto 4.1.1;
- Prima emissione registro dei trattamenti 4.1.2;
- consolidamento del registro dei trattamenti 4.1.2;
- prima emissione delle revisioni alle procedure aziendali di cui al punto 4.1.1;
- prima emissione valutazione dei rischi di cui al punto 4.1.3.

**Entro fine febbraio 2019:**

- consolidamento delle revisioni alle procedure aziendali di cui al punto 4.1.1;
- chiusura lavori.

## 8. CONDIZIONI GENERALI

A. Con la sottoscrizione della presente proposta il Cliente conferisce l'incarico a AVVERA, che accetta, di compiere le attività descritte nella proposta stessa.

B. La data di decorrenza della proposta verrà concordata tra Cliente e Avvera sulla base del piano di intervento condiviso.

C. I corrispettivi indicati in gara saranno pagati dal Cliente mediante bonifico bancario sul conto corrente intestato a AVVERA, presente in fattura, nei seguenti termini:

40% alla data di accettazione della proposta;
60% alla chiusura dei lavori.

Il pagamento dovrà essere effettuato entro 60 giorni dal ricevimento della fattura elettronica.

D. Per lo svolgimento dell'incarico, il personale di AVVERA dovrà avere pieno e libero accesso alle informazioni ed apparecchiature oggetto di intervento, che saranno tempestivamente e gratuitamente messe a disposizione del Cliente per i periodi di tempo necessari all'esecuzione dell'incarico stesso. Il Cliente garantisce la collaborazione del proprio personale al fine della buona riuscita dell'incarico.

E. Il Cliente è consapevole del fatto che la buona riuscita dell'incarico, che presume attività di accertamento, analisi e verifica, dipende dal fatto che al personale di AVVERA vengano comunicate informazioni e dati completi, pertinenti, veritieri e corretti.

F. Il Cliente potrà recedere dal presente Contratto a mezzo lettera raccomandata a.r., mantenendo indenne AVVERA delle spese sostenute, dei lavori eseguiti e del mancato guadagno, fermo restando che gli importi già pagati dal Cliente saranno trattenuti dalla stessa AVVERA.

G. AVVERA tratterà come strettamente confidenziale qualsiasi informazione espressamente indicata come tale dal Cliente, nonché manterrà il massimo riserbo su tutti i dati del Cliente e dei soggetti che operano con il Cliente di cui venisse a conoscenza nello svolgimento del servizio. Il trattamento operato sui suddetti dati sarà limitato alle sole operazioni strettamente necessarie ai fini dello svolgimento delle prestazioni oggetto del presente contratto.

H. Per effetto del presente accordo, il personale di AVVERA dedicato all'intervento è incaricato per iscritto da entrambe le parti ed è autorizzato a svolgere le sole operazioni di trattamento dei dati personali del Cliente e dei soggetti operanti con il Cliente (Interessati) strettamente necessarie a svolgere il proprio incarico, limitatamente al periodo di tempo necessario a concludere l'intervento oggetto del presente Contratto.

I. AVVERA sarà responsabile solamente dei danni di natura contrattuale ed extracontrattuale che costituiscono conseguenza immediata e diretta dei propri comportamenti determinati da dolo o colpa grave, con espressa esclusione pertanto di ogni danno indiretto, di ogni danno derivato a terzi dall'uso che il Cliente faccia dei risultati delle prestazioni al medesimo rese in forza del presente contratto, nonché di ogni danno cagionato in assenza di dolo o colpa grave. Il Cliente è tenuto, pena la decadenza da ogni azione, a comunicare per iscritto a AVVERA, a mezzo raccomandata a.r., qualsiasi rilievo o reclamo in merito al servizio reso entro e non oltre 1 mese dalla data di fine lavori. Salvo tutto quanto previsto dal presente punto I, in caso di responsabilità accertata di AVVERA il risarcimento è fin d'ora convenuto in una misura comunque non superiore al doppio dell'importo incassato per l'espletamento delle attività svolte.

J. Ai sensi dell'articolo 13 del Regolamento UE 2016/679 (GDPR), il Cliente è informato che i Suoi dati personali e quelli del personale di riferimento sono trattati da AVVERA per finalità di programmazione delle attività; gestione della clientela, adempimento di obblighi contabili e fiscali, gestione dei processi di qualità, gestione del contenzioso. Il trattamento è svolto mediante elaborazione elettronica con strumenti di office automation per il conseguimento delle predette finalità. I dati potranno essere comunicati per finalità di adempimento di obblighi di legge o contrattuali a banche (pagamenti), professionisti (commercialisti, ingegneri e avvocati). I dati saranno trattenuti per 10 anni, in funzione dell'obbligo di legge previsto dal codice civile e per scopi probatori. Il conferimento dei dati richiesti, siano essi acquisiti in base ad un obbligo di legge ovvero in quanto strettamente funzionali all'esecuzione del rapporto contrattuale, è necessario e l'eventuale rifiuto di fornirli comporta l'impossibilità di svolgere

le attività richieste per la conclusione e per l'esecuzione del contratto. In relazione al trattamento dei predetti dati il Cliente ed il suo personale, ai sensi del citato GDPR hanno il diritto di ottenere: a) la conferma dell'esistenza di dati personali che lo riguardano, la comunicazione in forma comprensibile dei medesimi dati e della loro origine, nonché della logica sulla quale si basa il trattamento; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge; c) l'aggiornamento, la rettificazione, la modifica, ovvero, qualora Vi abbia interesse, l'integrazione dei dati. Il Cliente ha inoltre il diritto di opporsi, per motivi legittimi, al trattamento dei dati personali che lo riguardano. Infine il GDPR prevede altresì i diritti di portabilità dei dati, nonché il diritto di limitare il trattamento. Tali diritti potranno essere fatti valere scrivendo al Titolare del trattamento: AVVERA SRL, largo Boccioni 1, 21040 Origgio (Va). L'interessato ha altresì diritto ad adire il Garante per la protezione dei dati personali.

K. Il presente Contratto annulla e sostituisce qualsiasi precedente accordo, intesa o contratto intervenuto tra le parti relativamente all'incarico conferito e costituisce l'integrale manifestazione di tutti gli accordi eventualmente intervenuti tra AVVERA ed il Cliente in ordine allo stesso oggetto. Qualsiasi modifica al presente Contratto dovrà risultare da atto validamente sottoscritto dai rappresentanti qualificati delle parti.

L. Per lo svolgimento delle attività di consulenza presso la sede del Cliente, il personale di AVVERA sarà munito di tesserini identificativi.

M. I rischi potenziali che il personale di AVVERA può portare all'interno dei luoghi di lavoro dei Clienti è limitato all'utilizzo del Personale Computer portatile, quindi ad un rischio di incendio per corto circuito del trasformatore e/o del PC stesso. Tali strumenti, oltre che possedere le relative marcature CE, sono mantenuti e controllati costantemente dalla nostra organizzazione, riducendo tale rischio potenziale ad un livello basso. a tal proposito il Cliente si impegna a segnalare al personale di AVVERA la conformità dell'impianto elettrico prima che vengano utilizzate le prese elettriche per ricaricare i pc portatili. in caso di sopralluogo in reparti produttivi, il Cliente si impegna ad avvisare preventivamente il responsabile del servizio prevenzione e protezione di avvera in merito ai rischi di salute e sicurezza dei lavoratori esplicitando anche la necessità di opportuni dispositivi di protezione individuale-dpi.

N. Il Cliente, al momento iniziale delle attività di consulenza e prima dell'ingresso del personale di AVVERA presso luoghi di lavoro di titolarità del Cliente stesso, fornirà al personale di AVVERA dettagliate informazioni sui rischi presenti nell'ambiente in cui essi si troveranno ad operare e sulle misure di prevenzione ed emergenza adottate in relazione all'attività svolta presso i medesimi luoghi di lavoro. Il Cliente garantisce che il personale di AVVERA, nell'esecuzione delle prestazioni di cui al presente contratto, dovrà essere sempre accompagnato da un addetto del Cliente.

O. Il Cliente vigilerà affinché il personale di AVVERA non utilizzi attrezzature, macchinari inclusi gli strumenti informativi di titolarità del Cliente stesso, che dovranno essere utilizzati esclusivamente dal personale del Cliente.

P. Avvera ha istituito il proprio modello di organizzazione, gestione e controllo per la prevenzione dei rischi di reato, ai sensi e per gli effetti del D. Lgs. 231/2001.

Q. Per qualsiasi controversia il Foro competente è esclusivamente quello di Milano qualunque sia il modo ed il luogo convenuti per il pagamento e l'esecuzione dell'Assistenza.

Per Accettazione del Cliente, lì

_____

FIRMA E TIMBRO DEL CLIENTE

Ai sensi e per gli effetti di cui all'art. 1341 e 1342 Cod. Civ. si approvano specificamente le clausole di cui agli articoli (8.I) Limitazioni responsabilità e decadenza e (8.Q) Foro esclusivamente competente.

_____

FIRMA E TIMBRO DEL CLIENTE