

ALLEGATO ESPLICATIVO

Allegato A) Servizio 1

Convenzione CONFINDUSTRIA CH-PE



CONFINDUSTRIA CHIETI PESCARA

REVISIONE	DATA EMISSIONE	DESCRIZIONE MODIFICA	REDATTO DA	VERIFICATO DA
0	05/06/2018	Prima emissione	Paolo Colleluori	DG



Sommario

1. Premessa	3
2. Fasi di sviluppo	4
2.1 Fase AS IS	4
2.2 Fase TO BE	4
2.3 Fase MAINTENANCE	4
3. Oggetto dell'offerta – Fase AS IS	5
3.1 INTERVENTO 1: Pre-Assessment	5
3.2 INTERVENTO 2: Assessment Tecnologico/Organizzativo	5
3.3 INTERVENTO 3: Report finale e presentazioni dei risultati	6
4. Durata del progetto	7
5. Effort	7
6. Figure professionali	7
7. Oneri richiesti al Cliente	7

1. Premessa

Il Regolamento generale sulla protezione dei dati (GDPR) impone nuove regole per le organizzazioni che offrono prodotti e servizi alle persone all'interno dell'Unione Europea (UE) o che raccolgono e analizzano dati relativi ai residenti nella stessa, indipendentemente dal luogo in cui si trovano.

I principali aspetti affrontati dal GDPR, prevedranno:

- Maggiori diritti in termini di privacy personale
- Maggiori doveri in termini di protezione dei dati
- Segnalazione obbligatoria delle violazioni
- Sanzioni severe in caso di non conformità

Il nuovo Regolamento Generale Europeo sulla Protezione dei Dati Personali n. 2016/679 (GDPR), entrato in vigore il 24 maggio 2016, con i suoi 99 articoli ha riscritto la disciplina della Privacy a livello europeo. L'entrata in vigore della normativa è prevista per il prossimo 25 Maggio 2018, ed i principali cambiamenti introdotti sono:

- Privacy personale
- Controlli e notifiche
- Criteri di trasparenza
- IT e Formazione



Privacy personale

Gli individui hanno il diritto di:

- Accedere ai propri dati personali
- Correggere errori nei propri dati personali
- Cancellare i propri dati personali
- Contestare l'elaborazione dei propri dati personali
- Esportare i dati personali



Controlli e notifiche

I responsabili del trattamento dei dati saranno tenuti a:

- Proteggere i dati personali con misure di sicurezza appropriate
- Segnalare alle autorità le violazioni dei dati personali entro 72 ore
- Ricevere l'autorizzazione prima di procedere all'elaborazione dei dati personali
- Conservare la documentazione dettagliata sull'elaborazione dei dati



Criteri di trasparenza

I responsabili del trattamento dei dati sono tenuti a:

- Fornire avvisi chiari sulla raccolta dati
- Evidenziare gli scopi dell'elaborazione e i casi di utilizzo
- Definire i criteri di conservazione e di eliminazione dei dati



IT e formazione

I responsabili del trattamento dei dati saranno tenuti a:

- Formare personale e dipendenti che si occupano di privacy
- Controllare e aggiornare i criteri relativi ai dati
- Avvalersi di un Responsabile della protezione dei dati (per le organizzazioni di grandi dimensioni)
- Creare e gestire i contratti responsabile del trattamento dei dati/fornitore

2. Fasi di sviluppo

I servizi e le attività consulenziali offerte dal Gruppo Xera, si articolano in 3 fasi:

- **Fase AS IS:** ASSESSMENT GDPR
- **Fase TO BE:** output della fase AS IS
- **Fase MAINTENANCE:** mantenimento anni successivi post TO BE

2.1 Fase AS IS

La prima fase, detta AS IS, è finalizzata ad un assessment organizzativo e tecnologico, per valutare il livello di maturità delle persone, dei processi e delle tecnologie aziendali, rispetto al GDPR.

Questa prima fase si articolerà nei seguenti 3 interventi:

- ✓ **PRE-ASSESSMENT**
- ✓ **ASSESSMENT TECNOLOGICO/ORGANIZZATIVO**
- ✓ **REPORT FINALE: REMEDIATION PLAN & ROAD MAP**

2.2 Fase TO BE

La seconda fase, detta TO BE, è finalizzata all'attuazione del remediation plan ed alla definizione di procedure tecniche ed organizzative, necessarie per conformarsi al nuovo Regolamento EUROPEO. Questa fase si articola nei seguenti interventi:

- ✓ **ADEGUAMENTI TECNOLOGICI ED ORGANIZZATIVO/PROCEDURALI**
- ✓ **FORMAZIONE AL PERSONALE AZIENDALE**
- ✓ **AUDIT INTERNO**

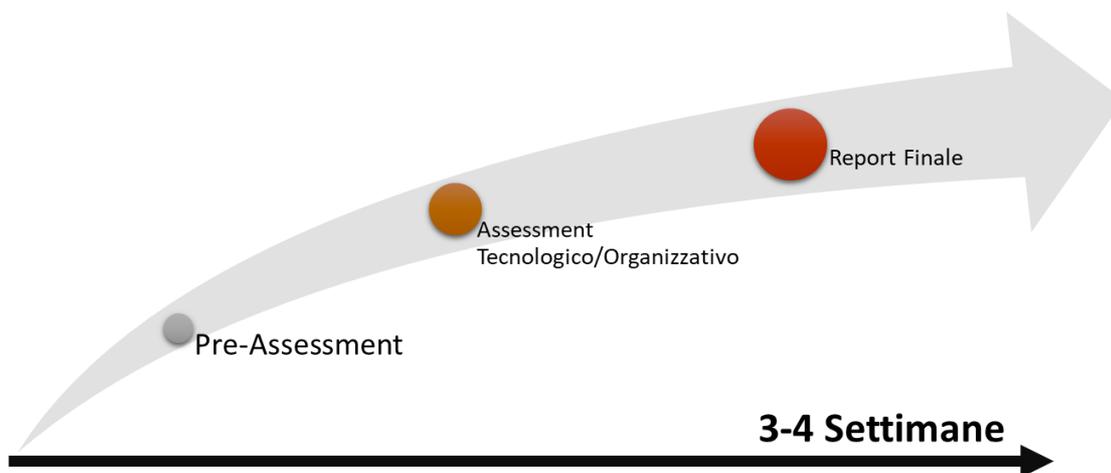
La fase TO BE è un output della fase AS IS, dunque è ovviamente indeterminabile sia a livello di azioni da svolgere che in termini di costi da sostenere in quanto viene pianificata a fronte di un assessment dettagliato che, conformemente a quanto definito dal Reg. UE si svolgerà con l'obiettivo di realizzare una valutazione dei rischi capace di focalizzare le priorità di intervento necessarie da un punto di vista tecnico – organizzativo per raggiungere la compliance. Il dettaglio dei servizi oggetto della presente offerta riguarda pertanto l'espletamento della fase AS IS. A conclusione di tale fase sarà discussa con la Direzione la volontà/opportunità di continuare ad avvalersi del Ns. supporto per il completamento della fase TO BE.

2.3 Fase MAINTENANCE

La terza fase, detta MAINTENANCE, è finalizzata a garantire il supporto periodico, la revisione ed il mantenimento del livello di compliance al Reg. EU, adeguando sistemi, procedure e metodi di lavoro rispetto alle evoluzioni tecnologiche, normative e aziendali. Questa fase si articola nei seguenti servizi:

- ✓ **SUPPORTO TECNICO/NORMATIVO ONLINE**
- ✓ **AUDIT ANNUALE DI VERIFICA E REVISIONE DEL LIVELLO DI COMPLIANCE**
- ✓ **SUPPORTO ALLA VERBALIZZAZIONE DEL RIESAME ANNUALE DEL SISTEMA**
- ✓ **AGGIORNAMENTO PERIODICO DELLA VALUTAZIONE DEI RISCHI E DI COMPLIANCE AL GDPR**
- ✓ **ASSUNZIONE DELL'INCARICO DI DPO (ove obbligatorio e richiesto dall'organizzazione)**
- ✓ **INDIVIDUAZIONE DEGLI ADEGUAMENTI TECNOLOGICI E SUPPORTO ALL'INTRODUZIONE NELL'ORGANIZZAZIONE**
- ✓ **INDIVIDUAZIONE DEGLI ADEGUAMENTI ORGANIZZATIVI E DOCUMENTALI**

3. Oggetto dell'offerta – Fase AS IS



3.1 INTERVENTO 1: Pre-Assessment

Tale fase sarà eseguita mediante l'effettuazione di un pre-engagement presso l'azienda finalizzato a:

- Illustrazione e presentazione del nuovo Regolamento Generale sulla Protezione dei Dati
- Pianificazione di un calendario di attività ed interventi
- Definizione dei ruoli e delle risorse aziendali, outsourcer e consulenti esterni coinvolti nell'assessment
- Collocazione dell'azienda rispetto al nuovo Regolamento Generale sulla Protezioni dei Dati

L'intervento avrà l'obiettivo di raccogliere le seguenti informazioni:

- Perimetro di analisi aziendale, con l'obiettivo di identificare la natura dei dati trattati, l'ambito di applicazione, il contesto e la finalità del trattamento
 - As IS rispetto all'impianto privacy ex D.Lgs 196/03.
 - Livello di iniziale di conoscenza del nuovo Regolamento Generale sulla Protezioni dei Dati

3.2 INTERVENTO 2: Assessment Tecnologico/Organizzativo

La fase di ASSESSMENT TECNOLOGICO/ORGANIZZATIVO, prevede un'attività di analisi dettagliata da effettuarsi presso il cliente con il coinvolgimento attivo delle risorse aziendali ed outsourcer, individuati nella fase di Pre-Engagement. L'obiettivo è quello di valutare il livello di maturità e compliance dell'azienda, rispetto al Regolamento GDPR. Questa fase verterà sulla raccolta di informazioni, finalizzate alla:

- Risk assessment
- Individuazione dei dati personali in possesso dell'azienda ed identificazione delle ubicazioni ed archiviazione e classificazione
- Identificazione delle attuali modalità di governance e trattamento dei dati
- Identificazione degli attuali livelli di sicurezza, protezione e vulnerabilità dei sistemi IT, di archiviazione e gestione dei dati
- Identificazione delle modalità di conservazione dei record e degli strumenti di reportistica in uso

La discovery dei dati con riferimento all' art. 4 del GDPR presenti su supporti informatici, potrà avvenire attraverso l'utilizzo di tools specifici laddove opportuno, e limitatamente al perimetro di intervento ed ai volumi e tipologie di dati individuati.

3.3 INTERVENTO 3: Report finale e presentazioni dei risultati

Ultima fase del servizio di consulenza riguarderà l'esecuzione delle seguenti attività:

- Redazione/revisione dei moduli/informative per il consenso alla raccolta e trattamento dei dati (informativa ai dipendenti, informativa ai clienti, informativa ai fornitori)
- Redazione template per la nomina dei responsabili del trattamento
- Redazione template per la nomina di "terzi autorizzati" al trattamento (ove previsto)
- Redazione del registro dei trattamenti dei dati
- Verifica requisiti e supporto nelle attività per la nomina del D.P.O (ove previsto)
- Verifica requisiti e stesura del Data Protection Impact Assessment – DPIA (ove previsto)
- Predisposizione del "Sistema di Gestione Privacy" così composto:
 - linee guida per monitoraggio e aggiornamento della mappatura e conseguente manutenzione del registro delle attività di trattamento;
 - organigramma egli incaricati del trattamento, formazione e monitoraggio;
 - scelta, designazione e monitoraggio dell'attività dei responsabili esterni;
 - Linee guida pe la gestione delle richieste di opposizione e limitazione del trattamento, accesso, rettifica, cancellazione dei dati e portabilità dei dati da parte dell'interessato, in modo tale che ciò avvenga in modo facile e senza ingiustificato ritardo;
 - Linee guida per il monitoraggio di eventuali violazioni dei dati subita;
 - Linee guida per la procedura di "Data Breach": notifica all'autorità garante e agli interessati in caso di violazioni
 - Linee guida per l'implementazione dei meccanismi di protezione dei dati che siano attivi fin dalla fase di progettazione delle attività (privacy by design) e per l'intera durata del trattamento e che siano trattati, di default, solo i dati personali necessari per ciascuna finalità specifica del trattamento.
 - Linee guida sulla sicurezza delle informazioni e sicurezza informatica (gestione degli utenti, delle password, degli accessi ecc...)

Le attività si concluderanno con un ultimo incontro in cui ci sarà la presentazione e condivisione con il Management aziendale dei seguenti elementi:

- livello di maturità e conformità complessivo dell'impianto organizzativo/tecnologico rispetto al GDPR
- livello di maturità e conformità specifico dell'impianto organizzativo/tecnologico rispetto alle macro aree di assessment (Discover, Manage, Protect, Report) del GDPR
- piano delle attività di remediation differenziate per area ORGANIZZATIVA/PROCEDURALE ed AREA TECNOLOGICA

4. Durata del progetto

La fase AS IS si sviluppa in un arco temporale di 4 settimane data contratto

5. Effort

Le attività si concretizzeranno in incontri pianificati c/o Vs. Sede con i responsabili di funzione per le attività di loro competenza ed in attività da svolgersi c/o i Ns. uffici.

Prima di ciascuna visita sarà Ns. cura informare preventivamente il Cliente delle attività che si andranno a svolgere e del personale che sarà coinvolto. La stima delle giornate sarà definita a fronte del primo incontro conoscitivo e di GAP ANALYSIS

6. Figure professionali

Denominazione	Sigla	Descrizione
Project Manager	PM-S	Figura professionale con esperienza pluriennale nella gestione di progetti di sviluppo di Hardware e Software di classe Enterprise. In particolare, per questa figura, è previsto l'utilizzo di personale con specifica esperienza in ambito editoriale.
Senior Privacy Consultant	PC-S	Figura professionale con esperienza pluriennale nella progettazione e implementazione di sistemi di gestione Privacy e risk management
Senior IT Consultant	IC-S	Figura professionale con esperienza pluriennale nell'analisi e progettazione di infrastrutture ICT, IT Security e Data Protection

7. Oneri richiesti al Cliente

Sarà Vs. cura:

- individuare un referente inteso come Vs. "braccio operativo" per la gestione degli incarichi che saranno di volta in volta definiti e come Ns. assistente continuo nel corso delle visite in azienda.
- fornire tutta la documentazione a Noi necessaria a supporto dei documenti del sistema privacy
- mettere a disposizione il personale da intervistare per le pertinenti funzioni ivi compresi eventuali outsourcer (es. Consulenti IT, Privacy, HR ecc..)