Data Protection Agreement (DPA) Titolare - Responsabile

I.R.P.E.T. – Istituto Regionale per la Programmazione Economica della Toscana (di seguito indicato con 'IRPET' o 'Titolare'), in qualità di Titolare del trattamento, nomina Maggioli spa (di seguito indicata con 'Società' o 'Responsabile'), quale Responsabile del trattamento, ai sensi dell'art 28 per lo svolgimento Regolamento (UE) n. 2016/679, per le prestazioni oggetto dell'affidamento del servizio di gestione documentale, che comportano il trattamento di dati personali per conto del Titolare

I trattamenti affidati con il presente atto dal Titolare al Responsabile riguardano l'espletamento delle attività oggetto dell'affidamento del servizio di gestione documentale, come definite nella lettera di invito (paragrafo 3, articolo 1) e nella lettera di affidamento, cui si fa integrale rinvio. Per il trattamento dei dati personali si richiama integralmente quanto previsto al paragrafo 3, art. 11.1, della lettera di invito. In particolare il Responsabile sarà chiamato a trattare i seguenti tipi di dati:

- dati comuni, dati anagrafici, dati personali comprensivi del codice fiscale, indirizzo di residenza, domicilio, numeri telefonici, e-mail, pec, del personale dell'Irpet e ad esso assimilabile ovvero dati comuni e di contatto (e-mail, pec) degli utenti/corrispondenti dell'Irpet;
- informazioni relative a dati comuni, dati anagrafici, personali e giudiziari, nonché - laddove previsto dalla normativa- dati sensibili afferenti la salute (es. certificati medici) o stati famigliari/personali, dati finanziari, contabili, fiscali presenti nei documenti ricevuti/inviati a/dal protocollo dell'IRPET, afferenti a titolo esemplificativo: la gestione del personale dipendente e assimilato dell'IRPET/procedure di selezione pubblica/conferimento incarichi o collaborazioni/ di nomina; procedure correlate a tirocini formativi/borse di studio/stage e visiting; procedure di gara/affidamento; stipula accordi di collaborazione/stipula contratti; gestione contabile/finanziaria/pagamenti e fatture; procedure di controllo del possesso dei requisiti soggettivi previste dalla normativa; procedimenti/provvedimenti autorità giudiziaria; ovvero ogni altro documento pervenuto e registrato al protocollo IRPET.

Tipologie degli interessati: lavoratori dipendenti e assimilati dell'IRPET; legali rappresentanti/amministratori di imprese/società/pubbliche amministrazioni/altri enti ed operatori privati ovvero individui che hanno rapporti di collaborazione/affidamento/contratti di qualsiasi tipo con IRPET, ovvero individui/utenti che partecipano a procedure/prestazioni/selezioni di qualsiasi tipo dell'IRPET ovvero che presentano istanze/richieste/comunicazioni al protocollo dell'IRPET.

Tipologia documento: testo, immagine, video, file, cartacei, documenti firmati digitalmente, cartelle, mail (ed ogni rappresentazione grafica ed fotografica ed elettromagnetica di atti e documenti).

Il trattamento dei dati avviene mediante applicativi informatici forniti e/o gestiti dal Responsabile del trattamento con modalità Saas. Le misure di sicurezza informatiche adottate per la gestione dei predetti applicativi sono indicate nell'offerta tecnica presentata dal Responsabile.

I trattamenti effettuati dal Responsabile per conto del Titolare e la presente nomina cesseranno al completamento del contratto ovvero in caso di sua risoluzione, per qualsiasi altro motivo.

Se una disposizione del presente atto è o diventa invalida o inapplicabile, la validità e l'applicabilità delle altre disposizioni del medesimo rimangono inalterate. In questo caso, Titolare e Responsabile

concordano di sostituire la disposizione invalida con altra disposizione idonea a raggiungere lo scopo originariamente prefissato o gli interessi comuni delle parti.

Nell'esercizio delle attività di trattamento che gli sono conferite dal Titolare, il Responsabile si impegna a rispettare la normativa vigente in materia di trattamento dei dati personali, con particolare riferimento a:

- Regolamento (UE) n. 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (di seguito Regolamento UE);
- Decreto Legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) come aggiornato dal Decreto Legislativo 10 agosto 2018, n. 101 (*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016*) (nel prosieguo Codice Privacy) e s.m.i..
- Provvedimenti del Garante della Privacy

La Società, in quanto Responsabile, fornisce garanzie sufficienti, in termini di conoscenze specialistiche, affidabilità e risorse, per attuare misure tecniche e organizzative che soddisfano i requisiti normativi sanciti dal Regolamento UE, dal Codice Privacy e da qualsiasi altra norma connessa inerente al trattamento dei dati personali, comprese le misure di sicurezza del trattamento, per assicurare la riservatezza e la protezione dei diritti degli interessati, come dalla stessa dichiarato in sede di offerta tecnica nella procedura di affidamento.

La Società, in quanto Responsabile, è tenuta ad assicurare e far assicurare ai propri dipendenti, collaboratori e responsabili ulteriori, la riservatezza ed il corretto trattamento delle informazioni, dei documenti e degli atti amministrativi, dei quali venga a conoscenza durante l'esecuzione della prestazione.

In tal senso il Responsabile, si impegna a consegnare al Titolare e al DPO di IRPET il "*Disciplinare di comportamento degli autorizzati e degli altri dipendenti*" coinvolti in modo e diretto o indiretto nell'esecuzione dei trattamenti svolti per conto del Titolare e delle istruzioni impartite agli autorizzati del Responsabile.

In particolare, ai sensi dell'art. 28 Regolamento UE, il Responsabile si impegna a:

1. Adottare e mantenere aggiornato un proprio registro dei trattamenti ai sensi dell'art. 30 del Regolamento UE.
2. Non mettere in atto, per nessun motivo, trattamenti di dati diversi da quelli autorizzati dal Titolare, oggetto del presente contratto e presenti nel registro dei trattamenti. In tal senso renderà accessibile al Titolare il registro dei trattamenti, attivati per effetto del contratto, consentendo

operazioni di consultazione, approvazione e diniego in relazione a singoli o gruppi di trattamenti.

3. Fornire per iscritto agli autorizzati al trattamento le necessarie istruzioni al riguardo.
4. Nominare gli autorizzati che svolgono le funzioni di "amministratore di sistema", ai sensi dei provvedimenti del Garante italiano per la protezione dei dati personali del 27/11/2008 e del 25/6/2009, conservando i relativi estremi identificativi, definendo gli ambiti di operatività ai medesimi consentiti e comunicandone al titolare l'elenco nominativo con i relativi ambiti di operatività.
5. Di collaborare alla eventuale redazione di DPIA su trattamenti affidati alla sua responsabilità dal Titolare.
6. Predisporre e trasmettere, su richiesta e comunque almeno una volta l'anno e ogni qualvolta ciò appaia necessario, al Titolare una relazione in merito agli adempimenti eseguiti e alle misure di sicurezza adottate al fine di renderle e mantenerle sempre adeguate ed aggiornate rispetto alla evoluzione delle minacce e sulla base dei riscontri derivanti dalla registrazione continua e puntuale degli incidenti eventualmente occorsi.
7. Assistere e garantire il Titolare del trattamento nell'evasione delle richieste e del rispetto dei tempi previsti, nei rapporti con l'Autorità Garante per la protezione dei dati personali.
8. Assistere il Titolare al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati ai sensi degli artt. 15 a 22 del Regolamento UE; qualora gli interessati esercitino tale diritto verso il Responsabile, quest'ultimo è tenuto ad inoltrare tempestivamente e comunque nel più breve tempo possibile, le istanze al Titolare, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei tempi prescritti.
9. Assistere ed assicurare la piena, fattiva e puntuale collaborazione al Titolare del trattamento, ed in particolare al Security IT Manager del Titolare, nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento, della tipologia di dati trattati, delle categorie e numerosità degli interessati.
10. Garantire al Titolare, su richiesta di questi, l'accesso e la disponibilità permanente ai dati, su formati e strumenti di uso comune che ne garantiscano la fruizione da parte del Titolare, consentendo in tal modo la piena continuità dei servizi oggetto del presente appalto e in modo che mai si configuri una situazione di "lock in". Il Titolare deve essere sempre messo in condizione di poter garantire la continuità del servizio.
11. Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento deve mettere in atto misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre, a titolo esemplificativo:

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

A tal fine il Responsabile si impegna ad assicurare la piena, fattiva e puntuale collaborazione al Titolare del trattamento ed al Security IT Manager del Titolare riguardo lo svolgimento delle seguenti attività:

1. Restituire tutti i dati personali di pertinenza del Titolare, dopo che sia terminata la prestazione dei servizi relativi al trattamento, cancellando le copie esistenti in proprio possesso, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati. In tal senso, entro 120 giorni dalla firma del contratto la Società e il responsabile del contratto per IRPET concordano modalità, tempi e forme idonee a garantire il non precostituirsi di situazioni di "lock in", inteso come la diminuzione o perdita della possibilità da parte del Titolare di garantire i servizi, senza ricorrere forzatamente al soggetto Responsabile, e di gestire agevolmente, in modo sicuro e con tempi ragionevoli, la chiusura del contratto e l'eventuale subentro di un nuovo contraente o la gestione in autonomia in toto o in parte dei servizi. Tale accordo documentato viene messo a disposizione del Titolare e del DPO di IRPET.
2. Informare tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. data breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quando il Titolare ne viene a conoscenza. Nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità di controllo siano esclusivamente in possesso del Responsabile e/o di suoi sub-Responsabili.
3. Consentire al Titolare l'adempimento all'obbligo di vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del trattamento, nonché di supervisionare l'attività di trattamento dei dati personali mediante l'esecuzione di audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile. A tal fine il Responsabile del trattamento metterà a disposizione, su richiesta del Titolare, tutte le informazioni necessarie per dimostrare il rispetto degli obblighi derivanti dal regolamento UE, agevolando il contributo alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro

soggetto da questi incaricato, e se necessario, l'attività di monitoraggio e di controllo da parte del DPO e del Security IT Manager sulle misure di sicurezza attuate e sulla loro efficacia fornendo tutta la documentazione che sarà richiesta e collaborando attivamente alle attività di rilevazione e misura.

4. Resta inteso che il Titolare avrà la facoltà di incaricare dei professionisti indipendenti per lo svolgimento di audit secondo standard internazionali e/o best practice, i cui esiti saranno riportati in specifici report ("Report"). Tali Report, che costituiscono informazioni confidenziali, potranno essere resi disponibili al Responsabile/Subresponsabile per consentirgli di verificare le eventuali azioni correttive da implementare in funzione al presente Accordo. Il Titolare dovrà previamente inviare richiesta scritta di Audit all'indirizzo del Responsabile. Successivamente alla richiesta di audit o ispezione, il Responsabile e il Titolare concorderanno, prima dell'avvio delle attività, i dettagli di tali verifiche (data di inizio e durata), le tipologie di controllo e l'oggetto delle verifiche (raccomandando l'utilizzo degli standard ISO 19011), i vincoli di riservatezza a cui devono essere vincolati il Titolare e coloro che effettuano le verifiche. Il Responsabile potrà opporsi per iscritto alla nomina da parte del Titolare di eventuali revisori esterni che siano concorrenti del Responsabile o che siano evidentemente inadeguati. In tali circostanze il Titolare sarà tenuto a nominare altri revisori o a condurre le verifiche in proprio. Restano a carico esclusivo del Titolare i costi delle attività di verifica dallo stesso commissionate a terzi..
5. Comunicare al Titolare i dati di contatto del proprio "Responsabile della protezione dei dati" (DPO), qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali (DPO) della Società (…indicare nome cognome e mail……) collabora e si tiene in costante contatto con il Responsabile della protezione dei dati (DPO) del Titolare.
6. Comunicare al Titolare, al DPO e al Security Manager i riferimenti di contatto del proprio Responsabile della sicurezza IT (Roberto Conci).
7. Porre in essere gli interventi necessari qualora dall'attività di monitoraggio e controllo emergessero punti di debolezza nelle misure tecniche e organizzative adottate o qualora durante l'esecuzione del contratto, la normativa in materia di trattamento dei dati personali generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.

8. Fornire e mantenere aggiornato il proprio catalogo degli asset (comprese le applicazioni utente e quelle di gestione dei sistemi e degli apparati), delle minacce e delle misure di sicurezza adottate e delle loro correlazioni.
9. Fornire al Titolare e al DPO, per il tramite del responsabile di contratto, il proprio piano di qualità di esecuzione della fornitura dei servizi, contenente le misure tecniche, organizzative e di processo al fine di fare fronte ai principi del Regolamento UE con riferimento particolare all'accountability, alla Data Protection by Design e by Default, alla tenuta del registro dei trattamenti, alla garanzia del rispetto dei diritti degli interessati di cui al Capo III del predetto Regolamento e alla consapevole responsabilizzazione del proprio personale coinvolto nel trattamento dei dati, che avviene per conto del Titolare.

Nel caso in cui il Responsabile ritenga opportuno avvalersi di ulteriori soggetti per lo svolgimento di prestazioni oggetto del presente contratto, che comportano il trattamento di dati personali è tenuto a:

- sottoporla a preventiva autorizzazione scritta e specifica del Titolare;
- nominare tali soggetti quali sub-Responsabili del trattamento, informando, con cadenza periodica semestrale, il Titolare del trattamento di ciascuna nomina e/o sostituzione dei detti sub-Responsabili; specificando nella comunicazione al Titolare le attività di trattamento delegate ed i dati identificativi del contratto stipulato con il sub-Responsabile del trattamento;
- far rispettare al sub-Responsabile obblighi analoghi a quelli che il Titolare gli ha attribuito, riportandoli nello specifico contratto o atto di nomina (tra lo stesso Responsabile e sub-Responsabile); qualora il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare la piena responsabilità dell'adempimento degli obblighi del sub-responsabile;
- far adottare agli eventuali sub-Responsabili, idonee e preventive misure di sicurezza tecniche ed organizzative appropriate, atte ad eliminare o, comunque, a ridurre al minimo qualsiasi violazione, rischio di distruzione o perdita, anche accidentale, dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme, nel rispetto delle disposizioni contenute nell'articolo 32 del GDPR.

Nel caso in cui i Responsabili agiscano in modo difforme o contrario alle legittime istruzioni impartite dal Titolare oppure adotti misure di sicurezza inadeguate rispetto al rischio connesso al trattamento effettuato, risponde del danno causato agli "interessati".

Resta inteso che, come previsto dall'art. 82 del GDPR, il Responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gki obblighi del presente atto specificamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare del trattamento.

In tal caso, il Titolare potrà risolvere il contratto, salvo il risarcimento del maggior danno dovuto.

Per tutto quanto non espressamente indicato nel presente articolo si rinvia al Regolamento UE n. 2016/679 sulla protezione delle persone fisiche ed al D.Lgs 30 giugno 2003 n. 196 e al D.Lgs 10 agosto 2018 n.101.

Per IRPET – il Titolare del trattamento
Nicola Sciclone, Direttore e Legale rappresentante
Firmato digitalmente

Per la Società – il Responsabile del trattamento
……, Procuratore Speciale
Firmato digitalmente