

Accordo sul trattamento e nomina a Responsabile del trattamento dei dati personali ("DPA")

ai sensi e per gli effetti dell'art. 28 del Regolamento (UE) 2016/679

*APPALTO PER L'ACQUISIZIONE DEI SERVIZI DI VULNERABILITY
ASSESSMENT/PENETRATION TEST E SECURITY CONSULTING*

CIG: 89122659BB

1. Salvo quanto necessario ai fini dell'esecuzione del presente Contratto, la sottoscrizione del Contratto e la fornitura dei Servizi oggetto dello stesso non comportano alcun accesso, uso o divulgazione di dati personali da parte dell'Appaltatore per conto della Committente, nè alcuna autorizzazione in tal senso.
2. Con la sottoscrizione del presente Contratto, l'Appaltatore è nominato Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE n. 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche "Regolamento UE"), per tutta la durata del Contratto, per quelle attività che dovessero comportare un trattamento di dati per conto della Committente, ai fini dell'esecuzione dei Servizi. A tal fine l'Appaltatore è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto del Contratto e si impegna ad effettuare, per conto della Committente, le sole operazioni necessarie per fornire i Servizi oggetto del presente Contratto, nei limiti delle finalità ivi specificate, nel rispetto del D.lgs. n. 196/2003 e s.m.i. e del Regolamento UE (nel seguito anche "Normativa in materia di trattamento dei dati personali") e delle istruzioni nel seguito fornite. Per le attività per le quali la Committente agisce a sua volta come responsabile del trattamento, la presente nomina deve intendersi quale nomina a sub-responsabile del trattamento ai sensi dell'art. 28 co. 4 del Regolamento.
3. La nomina a Responsabile del trattamento di cui al presente articolo ha durata pari a quella del presente Contratto.
4. L'Appaltatore si impegna a presentare, su richiesta della Committente, garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche ed organizzative adeguate volte ad assicurare che il trattamento sia conforme alle prescrizioni della normativa in tema di trattamento dei dati personali.
5. Le finalità per le quali il responsabile del trattamento è autorizzato a trattare i dati consistono nell'esecuzione delle attività e dei Servizi oggetto del Contratto.

6. I dati personali trattati in ragione delle attività oggetto del Contratto sono i dati a cui eventualmente potrebbe avere accesso l'Appaltatore nello svolgimento dei Servizi, inclusi a titolo esemplificativo e non esaustivo dati identificativi comuni e categorie particolari di dati.
7. Le categorie di interessati sono, a titolo esemplificativo e non esaustivo, personale in forze e collaboratori della Committente, utenti dei prodotti finali della Committente.
8. Nell'esercizio delle proprie funzioni, l'Appaltatore si impegna a:
 - a. rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del Contratto;
 - b. trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;
 - c. trattare i dati conformemente alle istruzioni impartite dalla Committente, che l'Appaltatore si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del Contratto, d'ora in poi "persone autorizzate"; nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE o delle altre disposizioni di legge relative alla protezione dei dati personali, l'Appaltatore deve informare immediatamente la Committente;
 - d. garantire la riservatezza dei dati personali trattati nell'ambito del presente Contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del presente Contratto:
 - si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
 - ricevano la formazione necessaria in materia di protezione dei dati personali;
 - trattino i dati personali osservando le istruzioni impartite dal titolare del trattamento per il trattamento dei dati personali;
 - e. adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (privacy by default);
 - f. adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;

- g. su eventuale richiesta della Committente assistere quest'ultima nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente all'articolo 35 del Regolamento UE, e nella eventuale consultazione del Garante per la protezione dei dati personali, prevista dall'articolo 36 del medesimo Regolamento UE;
 - h. ai sensi dell'art. 30 del Regolamento UE, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con la Committente e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione della Committente e dell'Autorità, laddove ne venga fatta richiesta ai sensi dell'art. 30 comma 4 del Regolamento UE.
9. Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, l'Appaltatore fornisce, entro 10 (dieci) giorni dalla sottoscrizione del presente Contratto e aggiorna nel tempo un piano di misure di sicurezza rimesso all'approvazione della Committente medesima, che saranno concordate in buona fede al fine di 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, se del caso:
- a. la pseudonimizzazione e la cifratura dei dati personali;
 - b. la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità dei dati personali e la resilienza dei sistemi e dei servizi che li trattano;
 - 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.
10. L'Appaltatore deve mettere a disposizione della Committente tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire alla Committente - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche, ispezioni e audit circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali. A tal fine, la Committente informa preventivamente l'Appaltatore con un preavviso minimo di 4 (quattro) giorni lavorativi.
11. Nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inadeguate ad assicurare l'applicazione del Regolamento, o risulti che l'Appaltatore agisca in modo difforme o contrario alle istruzioni fornite dalla Committente, quest'ultima diffiderà l'Appaltatore ad adottare tutte le misure più

opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 cc, la Committente potrà, in ragione della gravità della condotta dell'Appaltatore e fatta salva la possibilità di fissare un ulteriore termine per l'adempimento, risolvere il Contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

12. In alternativa alle verifiche di cui sopra, la Committente potrà richiedere all'Appaltatore di fornire annualmente o comunque su richiesta della Committente una relazione sull'andamento della gestione dei dati personali e sull'applicazione delle misure di sicurezza approvate.
13. L'Appaltatore può avvalersi di ulteriori sub-Responsabili per delegare loro attività specifiche, previa autorizzazione scritta della Committente, che non intende conferire autorizzazione generica alla nomina di sub-Responsabili.
14. Il sub-Responsabile del trattamento e/o terzo autorizzato del trattamento deve rispettare obblighi analoghi a quelli forniti dalla Committente all'Appaltatore, riportate in uno specifico contratto o atto di nomina. Spetta all'Appaltatore assicurare che il sub-Responsabile del trattamento e/o terzo autorizzato del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE.
15. In caso di violazione da parte del sub-Responsabile del trattamento e/o terzo autorizzato del trattamento degli obblighi in materia di protezione dei dati, l'Appaltatore è interamente responsabile nei confronti della Committente di tali inadempimenti. La Committente potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite audit verifiche e ispezioni anche avvalendosi di soggetti terzi. A tal fine, La Committente informa preventivamente l'Appaltatore con un preavviso minimo di 4 (quattro) giorni lavorativi.
16. Ove tali misure dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inadeguate ad assicurare l'applicazione del Regolamento, o risulti che il Sub-Responsabile agisca in modo difforme o contrario alle istruzioni fornite dalla Committente, quest'ultima diffiderà l'Appaltatore a far adottare al sub-Responsabile e/o ai terzi autorizzati del trattamento tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, resa anche ai sensi dell'art. 1454 cc, la Committente potrà, in ragione della gravità della condotta del sub responsabile e fatta salva la possibilità di fissare un ulteriore termine per l'adempimento, risolvere il contratto con l'Appaltatore ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

17. In alternativa alle verifiche di cui sopra, la Committente potrà richiedere all'Appaltatore di fornire annualmente o comunque su richiesta una relazione sull'andamento della gestione dei dati personali e sull'applicazione delle misure di sicurezza approvate da parte del sub-Responsabile.
18. L'Appaltatore si obbliga a manlevare e tenere indenne la Committente da qualsiasi perdita, contestazione, responsabilità, condanna o sanzione, nonché altre spese sostenute o dei costi subiti (anche in termini di danno reputazionale) per effetto di un'azione, reclamo, procedura intrapresa dal Garante privacy o da qualsiasi interessato qualora tale azione sia conseguenza anche di una sola violazione derivata dalla condotta attiva e/o omissiva dell'Appaltatore e/o dei suoi agenti e/o sub-contraenti della normativa in materia di trattamento dei dati personali, delle best practice in tema di sicurezza e/o delle obbligazioni assunte ai fini dell'esecuzione del presente Contratto, a titolo esemplificativo e non esaustivo il mancato o incorretto suggerimento di una mitigazione appropriata a una vulnerabilità rilevata nell'esecuzione dei Servizi.
19. L'Appaltatore deve assistere la Committente al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati; qualora gli interessati esercitino tale diritto presso l'Appaltatore, quest'ultimo è tenuto ad inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze alla Committente del Trattamento, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti.
20. L'Appaltatore informa la Committente tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, 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 (settantadue) ore da quando il titolare ne viene a conoscenza; nel caso in cui il titolare del trattamento debba fornire informazioni aggiuntive all'Autorità di controllo, l'Appaltatore si impegna a supportare la Committente o, se diverso, il Titolare del trattamento nell'ambito di tale attività.
21. L'Appaltatore deve avvisare tempestivamente e senza ingiustificato ritardo la Committente in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere la Committente nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del presente Contratto.
22. L'Appaltatore deve comunicare alla Committente il nome ed i dati del proprio "Responsabile della protezione dei dati", ove designato, comunicando tempestivamente alla Committente qualsiasi variazione; il Responsabile della

protezione dei dati personali dell'Appaltatore/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati della Committente.

23. Al termine della prestazione dei Servizi oggetto del contratto, l'Appaltatore su richiesta della Committente, si impegna a: i) restituire alla Committente i supporti rimovibili eventualmente utilizzati su cui sono memorizzati i dati; ii) distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione.
24. L'Appaltatore si impegna a individuare e a designare per iscritto gli amministratori di sistema mettendo a disposizione della Committente l'elenco aggiornato delle nomine.
25. L'Appaltatore si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i dati personali trattati in esecuzione del presente Contratto, siano precisi, corretti e aggiornati nel corso della durata del trattamento - anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati - eseguito dall'Appaltatore, o da un sub-Responsabile e/o terzo autorizzato.
26. L'Appaltatore non può trasferire i dati personali verso un Paese terzo o un'organizzazione internazionale salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte della Committente. In tal caso l'Appaltatore si obbliga a stipulare le Clausole Contrattuali Standard della Commissione Europea e a rispettare gli obblighi aggiuntivi che saranno eventualmente imposti, o le misure supplementari che saranno eventualmente richieste, dalla Committente. In ogni caso, l'Appaltatore assicura il rispetto delle misure di garanzie previste dal Regolamento EU e, a richiesta, ne fornisce prova alla Committente senza ritardo.
27. Sarà obbligo della Committente 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 dell'Appaltatore, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dall'Appaltatore.
28. Durante l'esecuzione del Contratto, nell'eventualità di qualsivoglia modifica della normativa in materia di Trattamento dei Dati Personali, di indicazioni del Garante privacy o dell'European Data Protection Board (EDPB) che generino nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), l'Appaltatore si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con la Committente e affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.



PagoPA S.p.A.
L'Amministratore Unico
Giuseppe Virgone
F.TO DIGITALMENTE

Per accettazione
L'APPALTATORE
F.TO DIGITALMENTE

