ZU_PIMS_MOD_SERVIZI INFORMATICI E PRIVACY

Autore	Ufficio Privacy
Approvazione	Mario Brocca

Versione Revisione

Versione	*Autore*	*Consultazione DPO*	*Data emissione*	*Motivo della revisione*
0.0	Ufficio Privacy		10/05/2018	Prima emissione
1.0	Ufficio privacy		14/05/2021	
2.0	Ufficio Privacy		23/09/2021	
3.0	Ufficio Privacy	24/07/2023	25/07/2023	Inseriti punti: 4.7 5.11 5.12 c) 6.2

PARERE DPO
ok

DESIGNAZIONE DI RESPONSABILE DEL TRATTAMENTO
- Data Processing Agreement -
(Art. 28 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016)

PREMESSO CHE

a. Tra il CLIENTE e il FORNITORE indicato nel contratto cui il presente documento si riferisce (di seguito FORNITORE) è in essere un contratto per l'erogazione di servizi informatici e/o servizi ad essi collegati (di seguito SERVIZIO e/o SERVIZI), di cui la presente è parte integrante;
b. nel presente contratto le parti concordano di definire
   - con il termine "GDPR" 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 e
   - con il termine "Normativa Privacy" le disposizioni del GDPR nonché tutte le altre disposizioni delle leggi dell'Unione o delle leggi degli Stati membri relative alla protezione dei dati personali e alla loro libera circolazione.
c. nello svolgimento del SERVIZIO, il Titolare del trattamento dei dati personali, ai sensi e per gli effetti dell'art. 4 co 1 n. 7 del GDPR, è il CLIENTE e incombe sullo stesso il compimento di tutti gli atti previsti dalla Normativa Privacy per il trattamento dei dati personali vale a dire l'informativa, la raccolta del consenso, l'adozione di tutte le misure autorizzative, di incarico e di conservazione e di altro tipo anche per realizzare il sistema sicurezza, ivi comprese le relative misure;

Ciò premesso, tra le Parti,

SI CONVIENE E SI STIPULA

quanto di seguito riportato.

1. Designazione di Responsabile del trattamento
   1.1. Per i compiti che, in base al contratto per il SERVIZIO, vengono affidati al FORNITORE, quest'ultimo ai sensi dell'art.4 co 1 n. 8) e dell'art. 28 GDPR è designato Responsabile del trattamento.
   1.2. Il Responsabile del trattamento precisa di essere in grado di offrire garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti degli interessati.

2. Oggetto del DPA
   2.1 Oggetto della presente designazione è definire le modalità e le condizioni contrattuali con le quali il Responsabile del trattamento si impegna ad effettuare, per conto del Titolare del trattamento, le operazioni di trattamento dei dati personali quali definiti dal contratto e specificate nell'allegato tecnico "Registro del trattamento del servizio" messo a disposizione a richiesta del Titolare del trattamento o consultabile nell'area riservata.
   2.2 Nel quadro delle loro relazioni contrattuali, le parti si impegnano a rispettare la regolamentazione in vigore applicabile al trattamento dei dati personali e, in particolare, il GDPR e la Normativa Privacy.

3. Durata del DPA
   La presente designazione avrà la durata del contratto a cui si riferisce.

4. Descrizione delle prestazioni del Responsabile del trattamento
   4.1 Il Responsabile del trattamento è autorizzato a trattare, per conto del Titolare del trattamento, dati personali necessari per fornire il SERVIZIO quale previsti dal contratto. Per i dati che il Titolare del trattamento ha già fornito e che fornirà, lo stesso garantisce di aver già acquisito il consenso degli interessati al loro trattamento ai sensi dell'art. 6 co 1 lett. a) l GDPR, salvi i casi indicati nel predetto art. 6 di trattamento consentito anche in assenza di consenso.
   Il Titolare del trattamento garantisce il Responsabile del trattamento di disporre legittimamente di tutte le informazioni che affiderà al Responsabile del trattamento per il loro trattamento, assicurando altresì che dette informazioni non violano in alcun modo diritti di terzi.
   Il Titolare del trattamento mantiene la titolarità delle informazioni che saranno comunicate al Responsabile del trattamento per il SERVIZIO ed assume espressamente ogni più ampia responsabilità in ordine al contenuto dei relativi dati personali e manleva il Responsabile del trattamento da ogni obbligo e/o onere di accertamento e/o di controllo diretto e indiretto al riguardo.
   4.2 La natura delle operazioni realizzate sui dati è l'erogazione del SERVIZIO e/o dei SERVIZI indicati nel contratto, per cui il Titolare del trattamento dichiara di affidare il relativo trattamento dei dati al Responsabile del trattamento.
   4.3 La finalità del trattamento, la natura e la tipologia dei dati trattati, le categorie di persone interessate sono quelle specificate nel "Registro del trattamento del servizio".
   4.4 Per quanto di sua competenza il Responsabile del trattamento, nel trattare i dati per l'erogazione del SERVIZIO, effettuerà il trattamento in osservanza dell'art. 5 GDPR relativo ai "Principi applicabili al trattamento dei dati personali".
   4.5 Per l'esecuzione dell'incarico oggetto del presente contratto, il Titolare del trattamento mette a disposizione del Responsabile del trattamento le informazioni necessarie all'esecuzione delle attività per il SERVIZIO, anche indirizzate all'utilizzo appropriato del sistema informativo.
   4.6 Il Responsabile del trattamento, ai sensi dell'art. 28 co 3 lett. b) GDPR, individua e incarica per iscritto le proprie persone autorizzate, definendo puntualmente l'ambito di trattamento consentito. Il Responsabile del trattamento si dichiara edotto che le proprie persone autorizzate agiscono sotto la sua autorità.
   4.7 Al fine di effettuare le attività di assistenza sugli strumenti del Cliente/Titolare del trattamento, quest'ultimo autorizza il Responsabile del trattamento a creare un collegamento permanente al relativo ambiente, con strumenti di teleassistenza, al fine di consentire la manutenzione del prodotto anche in mancanza di presidio degli addetti del Cliente.

5. Obblighi del Responsabile del trattamento
   Il Responsabile del trattamento, nello svolgimento delle sue funzioni, si impegna ad assolvere ed osservare i seguenti obblighi.
   5.1 Osservanza delle istruzioni date dal Titolare
   a. Il Responsabile del trattamento dovrà trattare i dati solo per le finalità sopra specificate e per l'esecuzione delle prestazioni contrattuali.
   b. Il Responsabile del trattamento dovrà trattare i dati in conformità a quanto previsto nel "Registro del trattamento del servizio" ed il Titolare del trattamento ritiene adeguate le misure di sicurezza ivi previste.
   5.2 Garantire la riservatezza
   a. Il Responsabile del trattamento garantisce l'osservanza della riservatezza dei dati personali trattati nell'ambito della presente designazione.
   b. Il Responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza e che esse ricevano e che venga loro data la formazione necessaria in materia di trattamenti dei dati personali.
   5.3 Adozione delle misure di sicurezza del trattamento
   a. Il Responsabile del trattamento deve procedere al trattamento dei dati personali in presenza delle misure richieste ai sensi dell'art. 32 GDPR. Le misure di sicurezza adottate sono quelle dichiarate nel "Registro del trattamento del servizio ". Il Titolare del trattamento prende atto che in alcuni casi il Responsabile del trattamento, procederà al trattamento attraverso gli

strumenti predisposti e configurati dallo stesso e pertanto dovrà adottare ogni cautela necessaria solo qualora il trattamento sia effettuato fuori dal controllo dello strumento impostato e configurato dal Titolare del trattamento.

b. Se il Responsabile del trattamento ha aderito ad un codice di comportamento, o ha esibito una certificazione, deve operare in presenza delle misure di sicurezza previste dal codice di comportamento o dai protocolli di cui alla certificazione. In questo caso il Titolare del trattamento accetterà la certificazione come prova del fatto che il Responsabile del trattamento ha adottato misure adeguate rispetto al trattamento effettuato, rinunciando ad effettuare attività di audit sui sistemi e sulle procedure del FORNITORE

c. Il Responsabile del trattamento, per i casi contemplati all'art. 37 del GDPR, opera avvalendosi del proprio Responsabile della protezione dei dati (RPT o DPO.): se designato, i riferimenti sono indicati nel "Registro del trattamento del servizio".

d. In conformità dell'art. 30 GDPR il Responsabile del trattamento (e, ove applicabile, il suo rappresentante, se non rientrante nei casi di esonero di cui al paragrafo 5 di tale articolo) deve tenere un registro di tutte le categorie di attività relative al trattamento svolte per conto del Titolare del trattamento, contenente quanto indicato nel co 2 di detto articolo.

e. I registri indicati sono tenuti in forma scritta, anche in formato elettronico, e saranno messi a disposizione del Titolare del trattamento a richiesta dello stesso e/o pubblicati nell'area riservata ai clienti.

5.4 Nomina di Sub responsabili

a. Ai sensi dell'art.28 co 2 GDPR, con la presente designazione, il Titolare del trattamento fornisce al Responsabile del trattamento espressa autorizzazione scritta generale alla individuazione di altri soggetti che svolgano, per conto del Responsabile medesimo, il ruolo di Sub-responsabili. A fronte di tale autorizzazione il Responsabile del trattamento si impegna a comunicare al Titolare del trattamento l'elenco di tutti gli eventuali soggetti individuati in qualità di sub-responsabili. Nel caso in cui nel tempo intervengano modifiche, aggiunte o sostituzioni dei sub-responsabili inizialmente comunicati, tali nuove nomine dovranno essere comunicate al Titolare del trattamento che avrà a disposizione 15 giorni per eventuali opposizioni. Il Responsabile del trattamento dichiara e garantisce che i Sub responsabili presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative idonee a garantire il rispetto delle disposizioni della vigente Normativa sulla Privacy e si impegna a vincolare contrattualmente gli ulteriori responsabili al rispetto degli stessi obblighi in materia di protezione dei dati personali assunti dal Responsabile del trattamento nei confronti del CLIENTE.

b. Qualora il Sub responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile del trattamento conserva, nei confronti del Titolare del trattamento, l'intera responsabilità dell'adempimento degli obblighi del Sub responsabile del trattamento.

c. Si precisa che, in tutti i casi in cui il SERVIZIO non sia erogato direttamente a favore del CLIENTE, ma a favore dei clienti finali dello stesso, il FORNITORE si configura come ulteriore Responsabile del trattamento, e sarà tenuto a trattare i dati alle medesime condizioni determinate nel presente atto di nomina per il Responsabile del trattamento."

5.5 Assistenza al Titolare per l'esercizio dei diritti degli interessati

a. Per quanto possibile, il Responsabile del trattamento – tenendo conto della natura del trattamento - deve assistere il Titolare del trattamento al fine di consentire allo stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III GDPR
Il Responsabile del trattamento, nella misura in cui ciò sia possibile, assisterà il Titolare del Trattamento con misure tecniche e organizzative adeguate.

b. In relazione al diritto di informazione degli interessati, spetta al Titolare del trattamento fornire l'informativa di cui agli artt. 13 e 14 GDPR alle persone interessate per le operazioni del trattamento, al momento della raccolta dei dati.

5.6 Assistenza al Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR

a. Il Responsabile del trattamento, tenendo conto della natura del trattamento e delle informazioni a sua disposizione, deve assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 del GDPR vale a dire:
   - l'articolo 32. Sicurezza del trattamento;
   - l'articolo 33. Notifica di una violazione dei dati personali all'autorità di controllo;
   - l'articolo 34. Comunicazione di una violazione dei dati personali all'interessato;
   - l'articolo 35. Valutazione d'impatto sulla protezione dei dati;
   - l'articolo 36. Consultazione preventiva.

b. Assistenza per la Sicurezza del trattamento - Il Responsabile del trattamento ha l'obbligo di assistere il Titolare del trattamento nella realizzazione della sicurezza del trattamento, conformemente all'art. 32 GDPR.
Il Responsabile del trattamento, a richiesta del Titolare del trattamento, relazionerà sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo, previa se necessaria valutazione a livello progettuale.

c. Particolari misure di sicurezza del Responsabile del trattamento già in atto - Il Titolare del trattamento prende atto che, per il SERVIZIO, il Responsabile del trattamento ha in essere misure di sicurezza adeguate in osservanza del GDPR.
Amministratori di sistema. In relazione alle attività svolte dal Responsabile del trattamento riferite alla conservazione dei dati personali e alle attività sistemistiche dirette alla manutenzione della rete e all'aggiornamento dei relativi data base e sistemi operativi, gli operatori del Responsabile del trattamento avranno la funzione di Amministratori di sistema.
Gli adempimenti previsti dal Garante per la privacy nel provvedimento del 27 novembre 2008 saranno gestiti dal Responsabile del trattamento; in particolare sarà il Responsabile del trattamento a valutare le caratteristiche soggettive degli amministratori di sistema, ad effettuare le designazioni individuali, a verificare le attività dagli stessi svolte ed a provvedere alla registrazione dei relativi accessi. In relazione a quanto previsto dal provvedimento stesso il Responsabile del trattamento si obbliga a comunicare al Titolare del trattamento l'elenco aggiornato degli Amministratori di sistema; la comunicazione di tali dati potrà avvenire in formato elettronico o cartaceo ed il Titolare del trattamento considera evaso tale adempimento anche con la semplice messa a disposizione dell'elenco aggiornato dei nominativi degli stessi Amministratori di sistema in un'area internet a ciò dedicata.

5.7 Assistenza per l'obbligo di Notifica di una violazione dei dati personali all'autorità di controllo
Il Responsabile del trattamento ha l'obbligo di assistere il Titolare del trattamento nell'adempimento dei propri obblighi di notifica di una violazione dei dati personali all'autorità di controllo, conformemente all'art. 33 GDPR. Il Responsabile del trattamento notifica al Titolare del trattamento ogni violazione di dati personali nel tempo massimo di 24 ore dopo esserne venuto a conoscenza. Tale notifica è accompagnata da quanto espressamente indicato nel 3 co dell'art. 33, utile per permettere al Titolare del trattamento, se necessario, di notificare questa violazione all'autorità di controllo competente.

5.8 Assistenza per l'obbligo di comunicazione di una violazione dei dati personali all'interessato
Il Responsabile del trattamento ha l'obbligo di assistere il Titolare del trattamento nell'adempimento degli obblighi di comunicazione di una violazione dei dati personali all'interessato, conformemente all'art. 34 GDPR; tale comunicazione andrà comunque sempre effettuata da parte del Titolare del trattamento.

5.9 Assistenza del Responsabile del trattamento, nell'adempimento dell'obbligo del Titolare del trattamento della valutazione d'impatto sulla protezione dei dati
Il Responsabile del trattamento assisterà il Titolare del trattamento nell'adempimento degli obblighi della valutazione d'impatto sulla protezione dei dati, conformemente all'art. 35 GDPR, fornendo ogni informazione utile in suo possesso attraverso il ""Registro del trattamento del servizio".

5.10 Assistenza del Responsabile del trattamento nell'adempimento dell'obbligo del Titolare del trattamento della consultazione preventiva
Il Responsabile del trattamento assiste il Titolare del trattamento nella consultazione preventiva dell'autorità di controllo, prevista dall'art. 36 del GDPR, fornendo al titolare ogni informazione utile in suo possesso attraverso il "Registro del trattamento del servizio".

5.11 Assistenza del Responsabile del trattamento nel caso di ispezioni/richieste da parte dell'autorità competente.

Il Responsabile del trattamento assiste e collabora con il Titolare del trattamento in caso di ispezioni/richieste da parte dell'autorità pubblica che possano in qualche modo riguardarlo.
In caso di ispezioni presso Il Responsabile del trattamento che riguardano il Titolare del trattamento, verrà data immediata comunicazione al Titolare del trattamento, qualora ciò sia possibile in relazione ai presupposti dell'indagine giudiziaria svolta.

5.12 Restituzione di tutti i dati personali al termine dell'incarico

a. Dopo che è terminata la prestazione dei servizi relativi al trattamento il Responsabile del trattamento, su scelta del Titolare del trattamento, dovrà restituire o cancellare tutti i dati personali e cancellare le copie esistenti.
I dati in possesso del Responsabile del trattamento dovranno essere restituiti al Titolare del trattamento, su richiesta dello stesso, attraverso la consegna del backup del data base o dei files su cui risiedono i dati personali; e/o cancellati entro i termini definiti nel "Registro del trattamento del servizio".
Eventuali ulteriori copie dei dati stessi di backup potranno essere conservate, per l'ulteriore periodo indicato nel "Registro del trattamento del servizio" per fini esclusivamente di sicurezza e non destinati alla comunicazione e alla diffusione
b. In deroga a quanto indicato ai punti precedenti, il Responsabile del trattamento dovrà conservare i dati nei casi in cui il diritto dell'Unione o degli Stati membri ne preveda la conservazione, nei termini imposti da detta normativa o da detti provvedimenti.
c. Qualora il Titolare inserisca nel sistema anche dati di altri Titolari del trattamento non firmatari del contratto, il Responsabile del trattamento non avrà alcuna responsabilità in riferimento a tali dati e le procedure di cancellazione e di backup saranno uniche e le sole previste per il Titolare firmatario. Ogni eccezione dovrà essere convenuta e gestita progettualmente al fine di determinarne gli effort economici

5.13 Messa a disposizione del Titolare del trattamento di tutte le informazioni necessarie per dimostrare il rispetto degli obblighi
Il Responsabile del trattamento metterà a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR e deve consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato – nei termini e nelle modalità meglio definite al successivo art. 8 – o dalle autorità.

5.14 Caso in cui un'istruzione al Responsabile del trattamento sia ritenuta in violazione del GDPR
Qualora, il Responsabile del trattamento, a suo parere, ritenga che un'istruzione del Titolare del trattamento violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati dovrà informare immediatamente il Titolare del trattamento.

5.15 Osservanza dei principi di "privacy by design" e di "privacy by default"
Il Responsabile del trattamento nello svolgimento dell'incarico dovrà operare in osservanza dei principi di protezione dei dati a partire da quando questi vengono progettati (privacy by design) e della protezione dei dati di default. L'identificazione dei requisiti di base dei sistemi e del rispetto di questi principi sarà definita su base progettuale in fase di start- up del servizio.

6. Obblighi del Titolare del trattamento

6.1 Il Titolare del trattamento deve:
- fornire al Responsabile del trattamento i dati previsti all'art. 4 delle presenti clausole;
- documentare per iscritto tutte le istruzioni riguardanti il trattamento dei dati da parte del Responsabile del trattamento;
- vigilare, in anticipo e durante la durata di tutto il trattamento, sul rispetto degli obblighi previsti dal regolamento europeo sulla protezione dei dati da parte del Responsabile del trattamento;
- supervisionare il trattamento, effettuando audit e ispezioni.

6.2 Qualora il sistema sia utilizzato da più aziende sarà responsabilità del Titolare del trattamento, firmatario del contratto, trattare in modo lecito i dati di tutti i Titolari del Trattamento ed il Fornitore gestirà il sistema e le attività accessorie collegate al contratto nei soli confronti del Titolare del trattamento firmatario

7. Luoghi ove sono e saranno custoditi i dati

7.1 I dati saranno trattati dal Responsabile del trattamento nei luoghi indicati nel "Registro del trattamento del servizio ". Qualora il trattamento dovesse essere eseguito in Paesi Extra UE, il Responsabile del trattamento metterà a disposizione del Titolare del trattamento le garanzie adottate in funzione del luogo in cui il trattamento sarà svolto.

7.2 Se il Responsabile del trattamento sarà tenuto ad effettuare un trasferimento dei dati verso un paese terzo o un'organizzazione internazionale, in virtù delle leggi dell'Unione o delle leggi dello stato membro al quale è sottoposto, deve informare il Titolare del trattamento circa tale obbligo giuridico prima del trasferimento al fine di ottenere autorizzazione, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

8. Controlli

8.1 Il Titolare del trattamento, si riserva, anche tramite verifiche periodiche, di vigilare sulla puntuale osservanza delle disposizioni di legge sul trattamento dei dati stessi e sul rispetto delle proprie istruzioni indicate nel presente documento. Il Responsabile del trattamento dovrà consentire al Titolare del trattamento, dandogli piena collaborazione, periodiche verifiche circa l'adeguatezza delle misure di sicurezza adottate e il rispetto della Normativa Privacy e delle disposizioni del Titolare del trattamento stesso.

8.2 Ogni attività di audit da parte del Titolare del trattamento dovrà essere convenuta con il Responsabile del trattamento, con un preavviso di almeno 10 giorni lavorativi. Qualora tali attività comportino oneri e spese non previste dal presente contratto tutte le richieste del Titolare del trattamento dovranno essere concordate nelle modalità di esecuzione e gestite a livello progettuale, con la definizione di una valutazione anche economica per la loro attuazione (siano esse attività di penetration test, vulnerability assessment, altro).