EHINET Srl - Gruppo ITER
Cap. Soc. 50.000 Euro i.v. - Iscrizione ROC n. 30236
Sede operativa: Via di Corticella, 181/3 - 40128 Bologna
Sede legale: Via Ugo De Carolis, 74 - 00136 Roma
Tel. 800 911 171 - (+39) 051 05 46 249 (Lun - Ven dalle 9 alle 19)
Fax 800 911 741 - (+39) 051 74 59 584 (24 ore su 24)
Sito: http://www.ehiweb.it

Data Processing Agreement per
LA DISCIPLINA DEL TRATTAMENTO DEI DATI PERSONALI IN QUALITA' DI RESPONSABILE DEL TRATTAMENTO AI SENSI DELL'ARTICOLO 28 DEL REGOLAMENTO UE 679/2016 (GDPR)

PREMESSA E DEFINIZIONI
Ai fini del presente Data Processing Agreement (di seguito "DPA"), "EHINET" è EHINET s.r.l. con sede legale in via Ugo De Carolis, 74 , 00136 - Roma - Capitale Sociale Euro 50.000,00 i.v. - iscritta al Registro Imprese di Roma - Partita I.V.A. e Codice fiscale 07931091008. "Cliente" il soggetto giuridico (persona fisica/persona giuridica) che opera in qualità di Titolare, Contitolare o Responsabile del trattamento.
I servizi prestati da EHINET al Cliente sono regolati dagli appositi contratti, dove vengono specificamente indicate le prestazioni fornite, secondo i termini e le condizioni contrattuali stabiliti nelle apposite Condizioni Generali di Servizio e relativo ordine da parte del Cliente (di seguito il "Contratto").
I termini adottati, inoltre, hanno il medesimo significato indicato nel Regolamento (UE) 2016/679 (d'ora in avanti, "GDPR") e nelle D.l.vo n. 196/2003.

Art. 1 - OGGETTO E SCOPO DEL DOCUMENTO
1.1 Il presente DPA ha ad oggetto modalità e condizioni di trattamento dei dati personali (d'ora in avanti, "Dati") di cui il Cliente è Titolare /Contitolare o che tratta in qualità di Responsabile del trattamento e rispetto ai quali nomina EHINET (di seguito definita solo "Fornitore"), responsabile del trattamento dei Dati dalla medesima effettuato in relazione al servizio fornito in esecuzione del Contratto in essere con il Cliente medesimo, di cui il presente DPA costituisce parte integrante.
1.2 In particolare, con il presente atto il Cliente nomina il Fornitore quale Responsabile esterno del trattamento in relazione al trattamento dei dati personali effettuato in occasione dell'erogazione dei servizi di cui al Contratto.
1.3 Pertanto il Fornitore effettuerà il trattamento dei dati personali in qualità di Responsabile esterno del trattamento (ai sensi dell'art. 4, 1° comma n. 8 del GDPR) ed il Cliente opererà in qualità di Titolare/Contitolare/Responsabile del trattamento dei dati personali (ai sensi dell'art. 4, primo comma, n. 7 del GDPR).
1.4 Ciascuna parte osserverà gli obblighi ad essa applicabili ai sensi GDPR e della legislazione nazionale applicabile in relazione al trattamento dei dati personali del Cliente.
1.5 Con il presente atto il Cliente incarica il Fornitore di elaborare i dati personali del Cliente solo in conformità con la legge applicabile: (a) per fornire i servizi richiesti dal Cliente; (b) come stabilito nel Contratto e nella ulteriore documentazione facente parte integrante del Contratto medesimo, comprese le presenti condizioni; e (c) come documentato ulteriormente in qualsiasi altra istruzione scritta fornita dal Cliente e riconosciuta dal Fornitore come costituente istruzioni ai fini del presente atto, purché conforme alle previsioni di legge.
1.6 Il Fornitore si atterrà alle istruzioni concordate nel presente documento. Il Cliente assicura al Fornitore il rispetto delle previsioni di legge in merito alla raccolta dei dati che saranno trattati nell'esecuzione dei servizi, ed, in particolare, di aver reso agli interessati le dovute informazioni richieste dalla normativa applicabile.
1.7 Nel caso in cui il Cliente mediante il Servizio effettui il trattamento di Dati a titolo diverso da quanto sopra indicato, dovrà darne apposita comunicazione scritta al Fornitore, che provvederà a contattare il Cliente per le opportune valutazioni del caso.
1.8 In ogni caso, qualora il Cliente effettui il trattamento dei dati personali in qualità di Responsabile il Cliente medesimo garantisce al Fornitore che le istruzioni e le azioni del Cliente in relazione a tali dati personali, compresa la nomina del Fornitore come altro Responsabile, sono state autorizzate dal Titolare del trattamento.
1.9 Il presente DPA non determina l'onere di prestare servizi ulteriori rispetto a quelli oggetto del Contratto intercorso tra il Cliente ed il Fornitore. Nel caso in cui il Cliente rilevi che il corretto adempimento degli oneri previsti dalla normativa applicabile richieda, anche in termini di sicurezza, l'erogazione di servizi o prestazioni aggiuntive il medesimo Cliente dovrà richiedere al Fornitore apposita quotazione economica per tali servizi o prestazioni che non potranno essere considerati automaticamente ricompresi all'interno di quelli espletati sulla base del Contratto.

Art. 2 - SICUREZZA
2.1 Il Fornitore, laddove applicabili, garantisce il rispetto delle misure di sicurezza indicate dalla normativa applicabile in materia di protezione dei Dati, nonché dai Provvedimenti dell'Autorità Garante con riguardo alle misure logiche, tecniche, fisiche ed organizzative che saranno poste in essere per proteggere i suddetti Dati da sottrazione o distruzione intenzionale o accidentale, perdita accidentale, alterazioni, uso non autorizzato, modifiche, divulgazione, diffusione, accessi non previsti e ogni altra forma di trattamento illecito.
2.2 Il Fornitore nell'erogazione dei Servizi applica le misure indicate nel Contratto, negli allegati tecnici, nell'Allegato "A" del presente atto e nelle procedure adottate, indicate al Cliente e messe in ogni momento a disposizione del medesimo.
2.3 Le misure di sicurezza comprendono misure per garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi del Fornitore; contribuire a ripristinare l'accesso tempestivo ai dati personali in seguito a un incidente e per test regolari di efficacia dei Servizi, il tutto secondo quanto descritto in via generale nell'Allegato "A" al presente atto. Il Fornitore può aggiornare o modificare le misure di sicurezza di volta in volta a condizione che tali aggiornamenti e modifiche non comportino il degrado della sicurezza complessiva dei Servizi.
2.4 Il Fornitore adotterà le misure appropriate per garantire la conformità con le misure di sicurezza da parte dei suoi dipendenti, appaltatori e Sub-responsabili relativamente al loro ambito di prestazioni.
2.5 Il Cliente riconosce che le misure tecniche ed organizzative adottate ed adottande dal Fornitore sono adeguate a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento dei Dati.
2.6 Il Fornitore provvederà a comunicare al Cliente, con i mezzi ritenuti più idonei, l'intervenuta modifica alle misure di sicurezza adottate per garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento dei Dati, anche in riferimento all'eventuale normativa che disciplina il servizio erogato. In tale ipotesi il Cliente avrà facoltà di richiedere un elenco aggiornato delle misure sicurezza specificamente adottate.
2.7 Il Cliente è l'unico responsabile per l'utilizzo dei Servizi, tra cui:

EHINET Srl - Gruppo ITER
Cap. Soc. 50.000 Euro i.v. - Iscrizione ROC n. 30236
Sede operativa: Via di Corticella, 181/3 - 40128 Bologna
Sede legale: Via Ugo De Carolis, 74 - 00136 Roma
Tel. 800 911 171 - (+39) 051 05 46 249 (Lun - Ven dalle 9 alle 19)
Fax 800 911 741 - (+39) 051 74 59 584 (24 ore su 24)
Sito: http://www.ehiweb.it

- fare un uso appropriato dei Servizi per garantire un livello di sicurezza adeguato al rischio in relazione ai Dati del Cliente;
- proteggere le credenziali, i sistemi e i dispositivi di autenticazione dell'account utilizzati dal Cliente per accedere ai Servizi
- effettuare il backup dei Dati del Cliente anche in via autonoma su apparati off-line.

2.8 Il Fornitore non ha alcun obbligo di proteggere i Dati del Cliente che il Cliente sceglie di archiviare o trasferire al di fuori dei sistemi del Fornitore e dei suoi Sub-reponsabili (ad esempio, lo spazio di archiviazione offline o locale) o di proteggere i Dati del Cliente implementando o mantenendo Controlli di sicurezza aggiuntivi rispetto a quelli descritti dal Contratto, dagli allegati tecnici e dall'Allegato "A".
2.9 Il Cliente è l'unico responsabile della valutazione del fatto che i Servizi, le misure di sicurezza e gli impegni del Fornitore ai sensi del presente articolo e di quanto previsto negli altri documenti contrattuali soddisfino le esigenze del Cliente, inclusi i suoi obblighi di sicurezza, anche ai sensi GDPR. Il Cliente riconosce ed accetta che (tenendo conto dello stato dell'arte, dei costi di implementazione e della natura, dell'ambito, del contesto e degli scopi del trattamento dei Dati personali del Cliente nonché dei rischi per gli individui) le misure di Sicurezza implementate e mantenute dal Fornitore forniscono un livello di sicurezza adeguato al rischio in relazione ai Dati del Cliente, impegnandosi a richiedere al Fornitore, sostenendone i relativi costi, eventuali misure di sicurezza aggiuntive qualora le ritenga necessarie in relazione alla tipologia di dati che saranno oggetto del trattamento e sollevando e manlevando il Fornitore da ogni e qualsiasi responsabilità in mancanza di tale richiesta.

Art. 3 – TRASFERIMENTO DI DATI
3.1 I Dati trattati dal Fornitore per l'erogazione dei Servizi, di cui al presente DPA, sono segregati a livello infrastrutturale. L'infrastruttura è ubicata nel territorio dell'Unione Europea presso i data center in cui vengono materialmente eseguite le procedure automatizzate per l'eventuale conservazione, duplicazione, backup e ripristino dei Dati.
3.2 In generale i Dati del Cliente non sono trasferiti in Paesi al di fuori dell'Unione Europea. Qualora sia necessario effettuare trasferimenti dei Dati verso tali Paesi il Fornitore provvederà a selezionare Paesi che siano stati già selezionati dalla Commissione Europea adeguati al livello di rischio, o a stipulare con il Sub-fornitore appositi contratti che contengano clausola standard, approvate dalla Commissione Europea, per la protezione dei Dati.

Art. 4 – ATTIVAZIONE ED EROGAZIONE DEI SERVIZI
4.1 Con la sottoscrizione del presente atto, il Cliente autorizza il Fornitore ad avvalersi di propri sub-responsabili riconoscendo ed accettando che ciò possa comportare il trattamento di Dati in favore dei medesimi.
4.2 Ai fini della nomina di un Sub-responsabile il Fornitore assicura tramite un contratto scritto che:
- il Sub-responsabile accede e utilizza i Dati del Cliente solo nella misura richiesta per adempiere alle obbligazioni al medesimo delegate in conformità con il Contratto;
- il Sub-responsabile assuma gli obblighi di cui all'art. 28 del GDPR;
- il Fornitore rimanga responsabile nei confronti del Cliente per tutti gli obblighi assunti, anche in relazione alle attività affidate al Sub-responsabile.

4.3 Al fine di consentire al Cliente, Titolare del trattamento dei Dati, un preciso controllo sui suddetti terzi, nonché di provvedere agli adempimenti sussistenti rispetto a tutta la categoria di detti terzi, Il Fornitore si impegna a conservare aggiornata la lista di tali soggetti terzi provvedendo su specifica richiesta scritta del Cliente ad esibire tale lista nonché apposita documentazione da cui risultino gli obblighi assunti da detti soggetti terzi in relazione agli oneri precisati nel presente DPA, qualora gli stessi trattino Dati in virtù dei servizi erogati.
4.4 Il Fornitore si impegna ad informare il Cliente, qualora richiesto, in caso di modifiche di tali soggetti terzi.

Art. 5 – VERIFICHE
5.1 Il Fornitore rende disponibile al Cliente tutte le informazioni necessarie per dimostrare la propria ottemperanza agli obblighi sulla protezione dei Dati imposti dalla normativa vigente in materia e dal presente DPA, purché le stesse non comportino l'analisi dei Dati di terze parti e non collidano con obblighi di riservatezza, anche in riferimento a segreti commerciali, assunti dal Fornitore.
5.2 Il Fornitore garantisce al Cliente, o ad altro soggetto da questi autorizzato, di poter effettuare verifiche circa la conformità del proprio operato agli impegni assunti nel presente DPA ed alla normativa vigente in materia di trattamento dei Dati, previo accordo sui tempi e sulle modalità di dette verifiche e purché le stesse non comportino l'analisi dei Dati di terze parti e non collidano con obblighi di riservatezza assunti dal Fornitore e con le policy del medesimo. I costi di tali verifiche saranno a carico del Cliente.
5.3 Il Fornitore si impegna a fornire tutte le informazioni necessarie a consentire al Cliente, Titolare del trattamento, di poter ragionevolmente verificare la conformità del medesimo Fornitore agli obblighi sulla sicurezza previsti dal Contratto e dal presente DPA.
5.4 Il Cliente dovrà autonomamente valutare la necessità o meno di effettuare una valutazione di impatto relativamente al trattamento dei dati, ai sensi dell'art. 35 del GDPR, comunicando tale necessità al Fornitore che, in tal caso, fornirà la propria assistenza per l'adempimento di tale obbligo.

Art. 6 – RICHIESTE DEGLI INTERESSATI
6.1 Qualora il Fornitore riceva durante il periodo di vigenza del Contratto una richiesta da un soggetto interessato relativa ai Dati personali, il Fornitore, se trattasi di Dati Personali gestiti per conto del Cliente informerà l'interessato di inviare la sua richiesta al Cliente ed il Cliente sarà responsabile di rispondere a tali richieste.
6.2 Nel caso in cui il Cliente non possa autonomamente fornire un riscontro secondo il precedente comma, il Fornitore si impegna a supportare il medesimo a riscontrare un'eventuale richiesta di accesso da parte degli interessati nella misura in cui ciò sia possibile e per quanto di propria competenza, secondo le modalità e le limitazioni previste nel presente DPA e della normativa applicabile.

EHINET Srl - Gruppo ITER
Cap. Soc. 50.000 Euro i.v. - Iscrizione ROC n. 30236
Sede operativa: Via di Corticella, 181/3 - 40128 Bologna
Sede legale: Via Ugo De Carolis, 74 - 00136 Roma
Tel. 800 911 171 - (+39) 051 05 46 249 (Lun - Ven dalle 9 alle 19)
Fax 800 911 741 - (+39) 051 74 59 584 (24 ore su 24)
Sito: http://www.ehiweb.it

6.3 Il Fornitore, compatibilmente con le specifiche tecniche fornite, dà al Cliente la possibilità di rettificare, cancellare, circoscrivere e/o recuperare i propri dati, nel rispetto delle condizioni concordate con il Cliente e della normativa applicabile.

Art. 7 – VIOLAZIONE DI DATI PERSONALI
7.1 Qualora si verifichino eventi che comportano la violazione dei Dati Personali trattati dal Fornitore nell'erogazione dei Servizi, quest'ultimo avvertirà il Cliente nel rispetto della normativa applicabile.
7.2 In particolare, il Fornitore informerà entro 24 ore dall'evento il Cliente. Tale comunicazione (i) descriverà la natura della violazione, compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione (ii) illustrerà le possibili conseguenze della violazione, (iii) esporrà le misure messe in atto o proposte dal Fornitore in risposta all'incidente e (iv) fornirà un punto di contatto presso il Fornitore.
7.3 È fatto obbligo di mantenere l'assoluto riserbo sulle violazioni, nonché su tutte le comunicazioni intercorse tra il Cliente ed il Fornitore a riguardo. Tali informazioni non dovranno essere in alcun modo diffuse in qualunque forma, anche mediante la loro messa a disposizione o consultazione. La comunicazione della violazione è ammessa solo tra il Cliente ed il Fornitore, fatte salve quelle comunicazioni richieste dalla legge o da autorità pubbliche.

Art. 8 - DURATA
8.1 Il presente DPA ha durata pari a quella del Contratto intercorso tra il Cliente ed il Fornitore. Il DPA cesserà automaticamente di avere efficacia in ipotesi di risoluzione, recesso o perdita di efficacia del Contratto, salvo il tempo eventualmente necessario a consentire al Cliente di recuperare i Dati Personali, come contrattualmente convenuto tra le parti.
8.2 Parimenti, in caso di tacito rinnovo del Contratto il presente DPA si considererà automaticamente rinnovato per durata pari a quella contrattuale

EHINET Srl - Gruppo ITER
Cap. Soc. 50.000 Euro i.v. - Iscrizione ROC n. 30236
Sede operativa: Via di Corticella, 181/3 - 40128 Bologna
Sede legale: Via Ugo De Carolis, 74 - 00136 Roma
Tel. 800 911 171 - (+39) 051 05 46 249 (Lun - Ven dalle 9 alle 19)
Fax 800 911 741 - (+39) 051 74 59 584 (24 ore su 24)
Sito: http://www.ehiweb.it

ALLEGATO "A"

MISURE DI SICUREZZA ADOTTATE DAL FORNITORE NELL'EROGAZIONE DEI SERVIZI ART. 32 DEL REGOLAMENTO (UE) N. 679/2016

Il presente Allegato riporta, in forma sintetica, le misure che il Responsabile del trattamento si impegna ad adottare per contrastare i rischi di sicurezza relativi ai trattamenti affidati. Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere (per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia), come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

Misure di Sicurezza	ADSL e FIBRA	VoIP	FAX	SMS	Hosting e VPS cloud	Server in co-location
Sistemi Antintrusione fisici	Sì, porte blindate					
Restrizione accessi alle sale server	Sì					
Armadi con serratura	Sì					
Locali chiusi a chiave	Sì					
Sistema Antincendio	Sì					
Sensibilizzazione e Formazione del Personale	Sì					
Vincoli di riservatezza sul personale	Sì					
Procedure organizzative	Sì					
Backup dei dati	N.A.	N.A.	N.A.	Sì	C	C
Sistemi di Autenticazione Informatica	Sì					
Firewall	N.A.	N.A.	Sì	Sì	C	C
Crittografia	Sì	N.A.	N.A.	Sì	C	C
Loggatura AdS	Sì	Sì	Sì	Sì	C	C
Aggiornamento/Patching Sistema Operativo	Sì	Sì	Sì	Sì	C	C
Aggiornamento/Patching Applicativo	Sì	Sì	Sì	Sì	C	C
Sistemi UPS	Sì					

EHINET Srl - Gruppo ITER
Cap. Soc. 50.000 Euro i.v. - Iscrizione ROC n. 30236
Sede operativa: Via di Corticella, 181/3 - 40128 Bologna
Sede legale: Via Ugo De Carolis, 74 - 00136 Roma
Tel. 800 911 171 - (+39) 051 05 46 249 (Lun - Ven dalle 9 alle 19)
Fax 800 911 741 - (+39) 051 74 59 584 (24 ore su 24)
Sito: http://www.ehiweb.it

Misure di Sicurezza	ADSL e FIBRA	VoIP	FAX	SMS	Hosting e VPS cloud	Server in co-location
Generatore elettrico	Sì					
High Availability	N.A.	N.A.	N.A.	N.A.	C	C
Disaster Recovery	N.A.	N.A.	N.A.	N.A.	C	C
Pseudonimizzazione	Sì	Sì	Sì	Sì	N.A.	N.A.

Legenda | C = ove previsto contrattualmente | N.A. = non applicabile | Sì = Prevista nel servizio di base

Per il Titolare del trattamento

Data: _____

Firma: _____

Per il Responsabile del trattamento

Data: _____

Firma: _____