Contratto per il Trattamento dei Dati Personali del Sub-Responsabile

INFORMAZIONI:

Title	Contratto per il Trattamento dei Dati Personali del Sub-Responsabile		
Date:	28/01/2019	**Version:**	1.2

I. PREAMBOLO

Premesso che:

A. Il Cliente, con riferimento ai servizi che fornisce ai propri clienti, agisce tipicamente come Responsabile del trattamento, mentre tali clienti, a seconda dei casi, agiscono come Titolari o come Responsabili del trattamento essi stessi;

B. Nel contesto della fornitura dei servizi, il Cliente può avvalersi di sub-responsabili per fornire tali servizi per suo conto. Laddove il Cliente agisce come Responsabile, tali sub-responsabili sono a loro volta considerati Responsabili del trattamento ai sensi del Regolamento (EU) 2016/679 (di seguito: "**GDPR**");

C. il Cliente intende regolare i rapporti con i propri sub-fornitori, in relazione ai trattamenti di dati personali, attraverso un accordo scritto in linea con i requisiti dell'art. 28 GDPR;

D. Il presente Contratto per il Trattamento dei Dati Personali, unitamente ai suoi Allegati (congiuntamente "**CTDP**"), viene sottoscritto tra il Cliente (di seguito: "**Cliente**" o "**Responsabile**"), i cui estremi identificativi sono riportati in calce al presente CTDP, e Register.it S.p.A. (di seguito: "**Register**" o "**Sub-Responsabile**"); il Cliente e Register, congiuntamente intesi come le "**Parti**", e ciascuno singolarmente come "**Parte**" al fine di riflettere gli accordi intercorsi tra le Parti con riferimento al Trattamento dei Dati Personali del Cliente, in osservanza delle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali.

E. Register ha convenuto di fornire il/i servizio/i ("**Servizio**") attivato/i dal Cliente alle condizioni contrattuali previste nel/negli Ordine/i di Servizio e nelle Condizioni Generali di Servizio complessivamente disponibili al link https://www.register.it/company/legal/ ("**Contratto Master**").

F. La tipologia, la natura e le finalità del Trattamento dei Dati Personali del Cliente relativo al Servizio, così come il tipo di Dati Personali e le categorie di Interessati, sono meglio descritti nell'Allegato 1 del presente CTDP.

G. Le Parti hanno concluso il presente CTDP al fine di assicurarsi la conformità alle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali e stabilire misure di sicurezza e procedure idonee per procedere al legittimo Trattamento dei Dati Personali del Cliente.

Il suddetto preambolo forma parte integrante del CTDP.

1. DEFINIZIONI

1.1 Salvo che sia diversamente definito nel presente CTDP, tutti i termini in maiuscolo utilizzati nel presente CTDP hanno il significato loro attribuito nel Contratto Master. In caso di contrasto o incongruenze per quanto riguarda la tutela della protezione dei dati tra il presente CTDP e il Contratto Master, prevale quanto stabilito nel presente CTDP.

“Autorità di Controllo” indica ogni autorità competente a vigilare ed assicurare l’applicazione delle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali con riferimento al Trattamento dei Dati Personali del Cliente svolti per mezzo del Servizio;

“Categorie Particolari di Dati Personali” indica i Dati Personali che rivelino: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il Trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

“Contratto Master” indica il contratto disciplinante la fornitura del Servizio concluso tra le Parti;

“CTDP” indica il presente contratto per il trattamento dei dati personali e gli Allegati 1, 2 e 3;

“Dati Personali del Cliente” indica i Dati Personali, relativi agli Interessati, Trattati in relazione al Servizio;

“Dati Personali” significa qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; al fine di evitare contrasti interpretativi, “Dati Personali” ha il significato previsto dal Regolamento e dalle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali;

“Diritti dell’Interessato” sono i diritti riconosciuti all’Interessato dalle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali. Nei limiti di applicabilità del Regolamento, “Diritti dell’Interessato” significa, ad esempio, il diritto di chiedere al Titolare l’accesso, la rettifica o la cancellazione dei Dati Personali, il diritto alla limitazione del Trattamento dei dati dell’Interessato o il diritto di opposizione al Trattamento, nonché il diritto alla portabilità dei dati;

"Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali" indica, negli Stati membri dell’Unione Europea, il Regolamento e le complementari legislazioni nazionali in materia di protezione dei Dati Personali, comprensivi di ogni orientamento e/o *code of pratice* emessi dalla competente Autorità di controllo all’interno dell’Unione Europea; e/o, negli Stati extra UE, ogni vigente legislazione in materia di protezione dei Dati Personali relativa alla tutela ed al legittimo Trattamento di Dati Personali;

“Elenco dei Sub-Responsabili” indica l’elenco disponibile inviando richiesta scritta a dpo@dada.eu;

“Interessato/i” ha il significato previsto dal Regolamento;

“Regolamento” o **"GDPR"** indica 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 che abroga la Direttiva 95/46/CE;

“Responsabile” indica generalmente la persona fisica o giuridica, la pubblica autorità, l’organismo o altro ente che Tratti Dati Personali per conto del Titolare. Ai fini del presente CTDP, il Responsabile è il Cliente e il Sub-Responsabile è la società Register.it S.p.A.;

“Servizio” indica il servizio oggetto del Contratto Master;

“Sub-Responsabile/i” indica un organismo individuato dal Responsabile per assisterlo nel (o che intraprenda direttamente qualsivoglia) trattamento dei Dati Personali del Cliente nel rispetto delle obbligazioni previste dal Responsabile e di cui al presente CTDP;

"Titolare" indica generalmente la persona fisica o giuridica, la pubblica autorità, l'organismo o altro ente che, da solo o congiuntamente con altri soggetti, determini le finalità e le modalità del Trattamento dei Dati Personali;

"Trattare" o **"Trattamento"** significa qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

"Violazione dei Dati Personali" indica la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati.

2. RUOLI PRIVACY

2.1. Le Parti convengono che:

a) il Cliente e Register agiscono entrambi come Responsabili con riferimento ai Dati Personali del Cliente nell'ambito dell'erogazione del Servizio;
b) I clienti ai quali il Servizio è fornito potrebbero agire come Titolari o come Responsabili per conto dei Titolari (es., clienti finali di tali clienti);
c) Register è stato incaricato dal Cliente di fornire il Servizio, per suo conto, ai clienti di il Cliente;
d) il presente CTDP regola il rapporto tra le Parti con riferimento ai rispettivi compiti e obblighi con riferimento al Trattamento dei Dati Personali del Cliente posto in essere dal Sub-Responsabile nell'erogazione del Servizio.

3. OBBLIGHI DEL SUB-RESPONSABILE

3.1. Il Sub-Responsabile si impegna a rispettare i seguenti obblighi, compresi quelli definiti negli Allegati 1, 2 e 3 che si considerano parte integrante del presente CTDP:

a) Il Sub-Responsabile tratterà i Dati Personali del Cliente solo per quanto strettamente necessario all'erogazione del Servizio, restando soggetto alle istruzioni impartite per iscritto dal Cliente e riflesse nel Contratto Master e nel presente CTDP;
b) Il Sub-Responsabile avvertirà il Cliente qualora ritenga che le istruzioni impartite per iscritto si pongano in violazione delle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali;
c) Il Sub-Responsabile informerà tempestivamente il Cliente, senza indebito ritardo, di ogni contatto o comunicazione ricevuta da un'Autorità di Controllo in relazione al Trattamento dei Dati Personali del Cliente.

d) Il Sub-Responsabile ha implementato misure operative, tecniche e organizzative adeguate ai sensi dell'art. 32 GDPR, incluse quelle descritte nell'Allegato 2 del presente CTDP, per proteggere i Dati Personali del Cliente. Le Parti sono consapevoli e concordano che il Sub-Responsabile è espressamente autorizzato ad implementare misure alternative o stabilire luoghi alternativi di conservazione dei dati purché il livello di sicurezza delle misure o dei luoghi scelti sia ritenuto, sotto tutti gli aspetti, adeguato.

e) Ove il Sub-Responsabile comunichi i Dati Personali del Cliente al proprio personale, direttamente ed esclusivamente preposto alla fornitura del Servizio, il Sub-Responsabile assicura che detto personale:

i) si è impegnato a mantenere la riservatezza o è soggetto ad un obbligo legale di riservatezza e;

ii) tratti i Dati Personali del Cliente seguendo le istruzioni del Cliente riflesse negli obblighi contenuti nel presente CTDP.

4. OBBLIGHI IN TEMA DI COLLABORAZIONE E RESPONSABILIZZAZIONE

4.1. Le Parti si impegnano a collaborare in buona fede per assicurare il rispetto delle previsioni di cui al presente CTDP e ad assistere i Titolari ad adempiere i loro obblighi derivanti dalle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali, tra cui, ma non solo, il dovere di assicurare il corretto e tempestivo esercizio dei diritti dell'Interessato, gestire incidenti di sicurezza/Violazioni dei Dati Personali al fine di mitigare i possibili effetti avversi da essi derivanti.

4.2 Le Parti collaborano in buona fede per rendere disponibile reciprocamente e ai Titolari, nonché verso le Autorità di Controllo, le informazioni necessarie a dimostrare il rispetto delle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali.

4.3 Il Sub-Responsabile si impegna a consentire ad audit e ispezioni sui sistemi e luoghi usati per il Trattamento dei Dati Personali del Cliente, condotte dal Cliente, dai Titolari o da auditor terzi inviati dal Cliente o dai Titolari, e a fornire la propria collaborazione. Gli audit e le ispezioni devono essere precedute da un ragionevole preavviso scritto nei confronti del Sub-Responsabile e non dovranno in ogni caso interferire con la normale operatività di business del Sub-Responsabile. Ogni informazione raccolta dovrà essere trattata in forma strettamente confidenziale, eccetto quando debbano essere rivelate in forza di norme cogenti (incluse, ma non solo, Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personal) o ordini delle autorità (inclusa, ma non solo, l'Autorità di Controllo).

5. AUTORIZZAZIONE AL TRATTAMENTO DEI DATI DA PARTE DI SUB-RESPONSABILI

5.1. Il Cliente riconosce, accetta ed acconsente che, esclusivamente per procedere alla fornitura del Servizio e nel rispetto di quanto stabilito nel presente CTDP, i Dati Personali del Cliente potrebbero essere Trattati da ulteriori sub-responsabili, come descritti nell'Elenco dei sub-responsabili.

5.2. Ai sensi dell'art. 5.1, Register è autorizzato a servirsi di ulteriori sub-responsabili a condizione che:
a) informi preventivamente il Responsabile dell'identità dei sub-responsabili come descritti nell'Elenco dei sub-responsabili e notifichi al Responsabile ogni aggiornamento del predetto elenco al fine di consentire al Responsabile di opporsi all'impiego di detti sub-responsabili;
b) stipuli accordi con sub-responsabili che contengano gli stessi obblighi previsti dal presente CTDP per quanto riguarda il Trattamento dei Dati Personali del Cliente;
c) eserciti adeguati controlli nel selezionare i sub-responsabili e rimanga responsabile per l'adempimento degli obblighi contenuti nel presente CTDP da parte dei sub-responsabili coinvolti;
d) su richiesta del Responsabile, il Sub-Responsabile fornisca al Responsabile adeguate informazioni in merito alle azioni ed alle misure che il Sub-Responsabile ed i suoi ulteriori sub-responsabili hanno intrapreso per assicurare il rispetto delle previsioni del presente CTDP.

6. DIRITTI DELL'INTERESSATO

6.1. In considerazione della natura del Trattamento, il Sub-Responsabile assiste il Cliente, con misure tecniche ed organizzative adeguate, nell'adempimento degli obblighi dei Titolari chiamati a riscontrare le richieste di esercizio dei diritti dell'Interessato.

6.2. Il Sub-Responsabile fornirà a il Cliente adeguata collaborazione ed assistenza e provvederà a fornire tutte le informazioni ragionevolmente richieste allo scopo di fornire riscontro all'Interessato o, altrimenti, per permettere al Titolare di dimostrare il rispetto dei propri doveri ed obblighi per quanto concerne i diritti dell'Interessato ai sensi delle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali.

7. RESTITUZIONE DEI DATI E CANCELLAZIONE

7.1. Fatto salvo quanto previsto dalla clausola 7.5, il Sub-Responsabile, senza porre costi aggiuntivi a carico del Cliente, a richiesta del Cliente restituirà i Dati Personali del Cliente (cancellando ogni copia dei Dati Personali del Cliente in suo possesso), oppure cancellerà i Dati Personali del Cliente senza ingiustificato ritardo e comunque non oltre trenta (30) giorni dalla ricezione della richiesta del Cliente.

7.2. Fatto salvo quanto previsto dalla clausola 7.5, alla scadenza o risoluzione anticipata del presente CTDP, il Sub-Responsabile, senza costi aggiuntivi per il Cliente, e/o su richiesta scritta del Cliente, restituirà i Dati Personali del Cliente (cancellando ogni copia dei Dati Personali del Cliente in suo possesso), senza ingiustificato ritardo e comunque non oltre trenta (30) giorni dalla scadenza o risoluzione anticipata del presente CTDP, a meno di diversa indicazione del Cliente.

7.3. Le Clausole 7.1. e 7.2 non si applicano nel caso in cui norme cogenti (incluse, ma non solo, Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personal) o ordini delle autorità (inclusa, ma non solo, l'Autorità di Controllo), impediscano al Sub-Responsabile di adempiere. Il Sub-Responsabile deve notificare al Cliente tali circostanze, fornendo un'adeguata giustificazione ed argomentando il proprio obbligo di conservare i Dati Personali del Cliente, senza ingiustificato ritardo e comunque non oltre dieci (10) giorni

dalla ricezione della richiesta del Cliente, o dalla scadenza o risoluzione anticipata del presente CTDP (a seconda dei casi). Il Sub-Responsabile rimarrà vincolato ai termini del presente CTDP (anche successivamente alla sua scadenza o risoluzione anticipata) rispetto ai Dati Personali del Cliente conservati secondo quanto previsto dalla presente cClausola, e gli è fatto divieto di Trattare in maniera attiva o intenzionale tali Dati Personali del Cliente per qualsivoglia finalità diversa dall'adempimento dei menzionali obblighi o ordini.

7.4. Quando i Dati personali del Cliente sono restituiti (essendo cancellata ogni copia dei Dati Personali del Cliente in possesso del Sub-Responsabile) o cancellati su richiesta del Cliente, in ottemperanza alle Clausole 7.1. e 7.2., il Sub-Responsabile dovrà rilasciare una dichiarazione scritta al Cliente, a conferma di tale restituzione o cancellazione, senza ingiustificato ritardo e comunque non oltre trenta (30) giorni dalla data in cui la restituzione o la cancellazione ha avuto luogo.

7.5. Il Sub-Responsabile potrà mantenere i Dati Personali del Cliente che siano stati conservati con regolari operazioni di backup nel rispetto dei protocolli di *disaster recovery* e *business continuity* del Sub-Responsabile (si veda art. 9), purché il Sub-Responsabile non compia, e non consenta ai propri sub-responsabili, di Trattare in maniera attiva o intenzionale tali Dati Personali del Cliente per qualsivoglia finalità ulteriore rispetto alla fornitura del Servizio. Il Sub-Responsabile rimarrà vincolato ai termini del presente CTDP (anche successivamente alla sua scadenza o risoluzione anticipata) rispetto ai Dati Personali del Cliente conservati secondo quanto previsto dalla presente Clausola.

8. VIOLAZIONE DEI DATI PERSONALI

8.1 Nel caso in cui il Sub-Responsabile venga a conoscenza di una Violazione dei Dati Personali, dovrà:

a) adottare le misure appropriate per contenere e mitigare tale Violazione dei Dati Personali, inclusa la notifica al Cliente senza ingiustificato ritardo dalla conoscenza della Violazione dei Dati Personali da parte del Sub-Responsabile;

b) cooperare con il Cliente e/o i Titolari per indagare la natura, le categorie ed il numero approssimativo di Interessati coinvolti, le categorie ed il numero approssimativo di Dati Personali coinvolti e le probabili conseguenze di tale Violazione con modalità commisurate alla serietà della Violazione ed al suo impatto complessivo sul Titolare e sull'erogazione del Servizio previsto dal Contratto Master;

c) ove le Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali richiedano la notificazione alle competenti Autorità di Controllo ed agli Interessati della Violazione dei Dati Personali, e nel caso essa si riferisca a Dati Personali del Cliente, il Sub-Responsabile dovrà deferire al, e prendere istruzioni dal Cliente e/o i Titolari; i Titolari saranno gli unici ad avere il diritto di determinare le misure che dovranno essere adottate per adempiere alle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali o per porre rimedio a qualsivoglia rischio, tra cui ma non solo:

i. determinare se l'avviso debba essere fornito a qualsivoglia individuo, autorità di regolamentazione, autorità giudiziaria, enti a tutela dei consumatori o altri come richiesto dalle

Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali, o richiesto a discrezione del Titolare; e

ii. determinare il contenuto di tale avviso, se sia possibile offrire all'Interessato dalla violazione qualche rimedio riparatorio, nonché la natura e l'ampiezza di tale rimedio.

9. DISASTER RECOVERY E BUSINESS CONTINUITY

9.1. Il Sub-Responsabile adotta e aggiorna, secondo criteri di diligenza professionale, protocolli di disaster recovery e business continuity, che differiscono a seconda del Servizio, la cui sintesi è resa disponile al Responsabile previa richiesta. Il Sub-Responsabile può modificare tale programma in qualsiasi momento, a condizione che la sua capacità di fronteggiare un disaster recovery non si riduca ad un livello inferiore a quello previsto dal suddetto programma al momento della sottoscrizione del presente CTDP.

Data, luogo _____

Il Cliente	Register.it S.p.A.
Nome e cognome / ragione sociale _____	
C.F. / P. IVA _____	C.F. / P. IVA 02826010163
(Firma) _____	(Firma) _____

ALLEGATO 1

1. INTERESSATI

I Dati Personali oggetto di Trattamento riguardano le seguenti categorie di Interessati (si prega di specificare):

☐ clienti e/o potenziali clienti

☐ fornitori

☐ dipendenti e/o potenziali dipendenti

☐ consulenti e/o professionisti

☐ altro (si prega di specificare):

_____

2. CATEGORIE DI DATI PERSONALI

I Dati Personali oggetto di Trattamento si riferiscono alle seguenti categorie di dati (si prega di specificare):

☐ dati di contatto (nome e cognome, indirizzo e-mail, indirizzo postale, numero di telefono)

☐ data di nascita

☐ età

☐ sesso

☐ altro (si prega di specificare):

_____

3. CATEGORIE PARTICOLARI DI DATI PERSONALI (OVE PRESENTI)

I Dati Personali oggetto di Trattamento si riferiscono alle seguenti Categorie Particolari di Dati Personali (si prega di specificare):

☐ disabilità e/o infortuni

☐ orientamento politico

☐ convinzioni etiche o religiose

☐ orientamento sessuale in cui è implicita la relazione o lo stato coniugale

☐ appartenenza sindacale

☐ stato di salute e/o malattie

☐ condanne penali e arresti

☐ altro (si prega di specificare):

_____

4. OPERAZIONI DI TRATTAMENTO

I Dati Personali potranno essere Trattati solo in relazione alla fornitura del Servizio così come descritto nel Contratto Master.

_____

ALLEGATO 2

Descrizione delle misure di sicurezza tecniche ed organizzative

Il Sub-Responsabile si impegna a garantire un livello di sicurezza non inferiore a quello previsto dalle misure tecniche e organizzative di seguito descritte.

Procedure sulla sicurezza delle informazioni

Organizzazione interna

Sono stati definiti ruoli e responsabilità separati per la sicurezza delle informazioni e sono stati assegnati alle persone autorizzate al trattamento dei dati personali della Società (di seguito anche "utenti") per evitare conflitti di interesse e prevenire attività inappropriate.

Sicurezza delle risorse umane

Dispositivi mobili e telelavoro

È prevista una Policy di sicurezza per l'utilizzo di tutti i dispositivi aziendali, in particolare quelli mobili, e sono in essere adeguati controlli.

Conclusione o modifiche al rapporto di lavoro

Al momento dell'uscita di un utente dall'organizzazione o nel caso di modifica significativa del ruolo ricoperto i permessi di accesso vengono aggiornati immediatamente, gli strumenti aziendali restituiti e azzerati sia fisicamente che logicamente.

Gestione delle risorse del patrimonio aziendale

Responsabilità delle risorse del patrimonio aziendale

Tutte le risorse del patrimonio aziendale sono accuratamente inventariate ed è monitorata l'assegnazione delle stesse ai vari utenti che sono responsabili per la loro sicurezza. È definita una policy per l'uso corretto delle stesse.

Classificazione delle informazioni

Le informazioni sono classificate e catalogate dai rispettivi utenti in linea con quanto previsto dalle esigenze di sicurezza, nonché trattate in modo appropriato.

Gestione dei media

Le informazioni conservate sui media sono gestite, controllate, modificate ed utilizzate in modo tale da non comprometterne il loro contenuto e sono cancellate in modo adeguato.

Controllo degli accessi

Requisiti aziendali per il controllo degli accessi

I requisiti organizzativi aziendali per il controllo degli accessi alle risorse informative sono documentati in una *policy* e in una procedura di controllo degli accessi; l'accesso alla rete ed alle connessioni è limitato.

Gestione dell'accesso degli utenti

L'allocazione dei diritti di accesso agli utenti è controllata dalla registrazione iniziale dell'utente fino alla rimozione dei diritti di accesso quando non più necessari, incluse le speciali restrizioni per i diritti di accesso privilegiato e la gestione delle "informazioni segrete di autenticazione", ed è soggetta a revisioni e controlli

periodici incluso aggiornamento dei diritti di accesso. Nella gestione degli accessi viene utilizzato il criterio della minimizzazione dei diritti di accesso, che sono rilasciati al fine di permettere all'utente l'accesso ai soli dati necessari per la sua attività. Diritti di accesso ulteriori richiedono una specifica autorizzazione.

Responsabilità degli utenti

Gli utenti sono consapevoli delle loro responsabilità anche attraverso il mantenimento di un effettivo controllo degli accessi, ad esempio scegliendo una password complessa, complessità comunque verificata dal sistema, e tenendola riservata.

Sistemi e applicazioni per il controllo degli accessi

L'accesso alle informazioni è soggetto a restrizioni nel rispetto della *policy* sul controllo degli accessi, attraverso un sistema di accessi sicuri e di gestione delle password di accesso oltre al controllo sulle utilità privilegiate e l'accesso limitato a tutti i codici sorgente.

Crittografia

Controllo crittografico

È in essere una Policy sull'uso della cifratura dei supporti e dei dati degli utenti. Le autenticazioni sono criptate.

Sicurezza fisica e ambientale

Sono in essere misure di sicurezza fisica e ambientale volte a prevenire l'accesso, la perdita o la diffusione illegittima o accidentale dei dati presenti nelle varie strutture.

Aree sicure: data center

I servizi della Società vengono erogati e ospitati in più data center nel mondo, tra i quali uno dei principali per la custodia dei dati personali dei clienti è tra i pochi data center in Italia certificati Tier IV, ossia la massima garanzia che un data center possa offrire. Tutti i data center all'interno della catena di fornitura offrono ridondanza completa di tutti i circuiti elettrici, di raffreddamento e di rete. Tutti i data center dispongono di illuminazione perimetrale oltre ad un sistema di rilevamento di presenza con telecamere a circuito chiuso; le porte di emergenza sono dotate di allarme. Tutti gli allarmi sono concentrati in control room.

L'accesso fisico è regolato e controllato da procedure di autorizzazione, riconoscimento e registrazione ed è circoscritto, grazie al sistema di controllo accessi, alle aree per le quali si è in possesso di autorizzazione.

Apparecchiatura

È in essere una policy per lo smaltimento delle apparecchiature dismesse in modo da distruggere in modo sicuro tutte le informazioni contenute.

Sicurezza delle operazioni

Procedure e responsabilità operative

Le responsabilità operative in ambito IT sono documentate e le modifiche alle strutture ed ai sistemi IT sono controllate. I sistemi di sviluppo, quelli di verifica e quelli operativi sono separati. Sono definiti utenti responsabili del corretto funzionamento delle procedure. E' invece a cura del cliente dei singoli servizi della Società (di seguito anche, il "cliente") la gestione della sicurezza logica dei sistemi operativi e delle applicazioni installate dal cliente.

Protezione da malware

È attivo sui device aziendali il controllo dei virus e dei malware, e c'è un'idonea consapevolezza sul punto da parte degli utenti.

Con riguardo ai servizi di Server Virtuale o Server Dedicato è a cura del cliente l'installazione di antivirus e anti malware e - se non è stato acquistato il relativo servizio - di firewall. Con riguardo al servizio di Hosting è invece in essere una protezione in real-time sulle macchine di front-end.

Con riguardo al servizio e-mail il traffico di posta viene analizzato in tempo reale, sia in ingresso che in uscita, per il rilevamento di virus, malware e per l'identificazione e il filtraggio dello spam. L'analisi è automatica e si basa sia sulla natura del contenuto, sia sulla interrogazione di basi dati internazionali, sia sulla reputazione acquisita grazie a una serie di parametri.

Backup

Vengono eseguiti backup periodici, ad esclusione dei servizi per i quali è responsabilità del cliente effettuare e gestire i backup (Server Dedicati e Server Virtuali). Per i servizi di Hosting e Posta vengono effettuati backup periodici che, per i servizi di Hosting, possono essere acceduti anche dal cliente. Ulteriori backup, non accessibili dai clienti, vengono effettuati a solo scopo di Disaster Recovery

Autenticazione e monitoraggio

Autenticazione e sincronizzazione

Ogni attività ed evento relativo alla sicurezza delle informazioni da parte degli utenti del sistema e degli amministratori/operatori avviene previo inserimento delle credenziali di autenticazione o certificati di identità. Gli orologi di tutte le apparecchiature sono sincronizzati.

Controllo di software operativi

L'installazione di software sui sistemi operativi è controllata e monitorata.

Con riguardo ai Server Virtuali ed ai Server Dedicati i sistemi operativi rilasciati ai clienti vengono resi disponibili con immagini di installazione aggiornate anche in fase di installazione a cura del cliente. È parimenti a cura del cliente l'eventuale aggiornamento del firmware ed anche delle applicazioni o software installati dal cliente.

Gestione delle vulnerabilità tecniche

Patch management

Ogni vulnerabilità tecnica viene corretta con idonee patch e sono previste procedure per tutte le fasi di test e per la conseguente installazione dei software e degli aggiornamenti che avviene solo quando tutti i test sono positivi.

Considerazioni sull'audit per le informazioni di sistema

Vengono effettuate verifiche periodiche al fine di controllare che siano ridotti al minimo gli eventuali effetti negativi sui sistemi di produzione e che non vi siano accessi abusivi ai dati.

Sicurezza delle comunicazioni

Gestione della sicurezza della rete

Le reti e i servizi in rete sono resi sicuri anche attraverso la loro separazione e la segregazione.

Trasferimento delle informazioni

Sono in vigore accordi relativi al trasferimento delle informazioni da e verso terze parti.

Acquisizione, sviluppo e manutenzione del sistema

Sicurezza nello sviluppo e processi di supporto

Le regole che governano la sicurezza dello sviluppo dei software e dei sistemi sono definite in una Policy. Le modifiche al sistema (sia per le applicazioni che per i sistemi operativi) sono controllate. La sicurezza del sistema è testata e sono definiti criteri di ammissibilità che includono gli aspetti di sicurezza.

Rapporti con i fornitori

Sicurezza delle informazioni nei rapporti coi fornitori

Sono previsti contratti o accordi volti a proteggere e a disciplinare il trattamento delle informazioni dell'organizzazione e dei clienti che siano accessibili a soggetti terzi operanti nell'area IT e ad altri fornitori terzi presenti nell'intera catena di fornitura.

Gestione dei servizi resi dal fornitore

L'erogazione dei servizi resi dai fornitori viene monitorata e verificata in relazione al contratto o all'accordo. Ogni modifica al servizio viene controllata.

Gestione degli incidenti alle informazioni di sicurezza

Gestione degli incidenti alla sicurezza delle informazioni e miglioramenti

Sono previste responsabilità e procedure apposite volte a gestire in modo coerente ed efficace gli eventi e gli eventuali incidenti relativi alla sicurezza delle informazioni (ad es. procedura di cd. Data Breach).

Aspetti della sicurezza delle informazioni relativi alla continuità aziendale

Ridondanze

Tutte le principali strutture IT sono ridondate per soddisfare i requisiti di disponibilità. Laddove questa ridondanza non è in essere, sono in atto adeguate misure per garantire la continuità del servizio o la riduzione al minimo della perdita di dati.

Conformità

Conformità ai requisiti legali e contrattuali

L'azienda identifica e documenta i suoi obblighi verso le autorità esterne e le altre terze parti in relazione alla sicurezza delle informazioni, compresa la proprietà intellettuale, la documentazione contabile e le informazioni relative alla privacy.

Revisione della sicurezza delle informazioni

I progetti dell'organizzazione relativamente alla sicurezza delle informazioni e le policy di sicurezza sono revisionate e vengono promosse azioni correttive ove necessario.

ALLEGATO 3 **(Elenco dei sub-responsabili)**

L'Allegato 3 (Elenco dei sub-responsabili) va richiesto scrivendo a dpo@dada.eu.