ALLEGATO – MISURE DI SICUREZZA

Il RTI si impegna a rispettare, nello svolgimento dei Servizi oggetto del Contratto, le seguenti Misure di sicurezza definite e concordate tra CDS e il RTI stesso. L'obiettivo è adottare idonee misure tecniche ed organizzative al fine di implementare un livello di sicurezza adeguato al rischio legato al trattamento dei dati personali e nel rispetto degli obblighi di cui all'art. 32 del Regolamento UE.

Requisiti di sicurezza GDPR

Nel caso di trattamento di dati personali del titolare da parte di uno dei componenti del RTI, durante lo svolgimento delle attività del contratto di appalto, le seguenti misure di sicurezza sono da considerarsi obbligatorie:

Legittimità del trattamento

- trattare i dati personali per le sole finalità specificate nel contratto e nei limiti dell'esecuzione delle prestazioni contrattuali;
- trattare i dati personali conformemente alle istruzioni impartite dal Titolare. Il RTI si impegna a far osservare le istruzioni alle persone autorizzate ad effettuare il trattamento dei dati personali oggetto del contratto. Nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali, il RTI deve informare immediatamente il Titolare del trattamento.

Riservatezza dei dati personali

- garantire la riservatezza dei dati personali trattati nell'ambito del contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del 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 per il trattamento dei dati personali;
  - qualora vi dovesse essere richiesta di aggiunta, modifica o cancellazione di un dato, questa venga ricevuta solo attraverso un processo formale, atto ad autorizzare gli incaricati alle relative operazioni sui sistemi. Tale processo sarà definito tra l'Amministrazione ed il RTI;
  - qualora arrivassero richieste non conformi con quanto concordato nel contratto, non si proceda con le operazioni richieste;
- adottare misure organizzative adeguate a 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.

Registro dei Trattamenti

- ai sensi dell'art. 30 del Regolamento UE, e nei limiti di quanto esso prescrive tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità, per le sole attività e quindi trattamenti di dati personali in carico ad RTI, e cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione del Titolare e dell'Autorità, laddove ne venga fatta richiesta ai sensi dell'art. 30 comma 4 del Regolamento UE.

Data Protection Impact Analysis (DPIA)

- assisterà il Titolare nello svolgimento della valutazione d'impatto sulla protezione dei dati per le attività e quindi per i trattamenti rientranti nel Contratto, conformemente all'articolo 35 del Regolamento UE e nella eventuale consultazione del Garante per la protezione dei dati personali, prevista dall'art. 36 del medesimo Regolamento UE.

Conservazione dei dati personali

- seguirà le istruzioni del Titolare in merito alla conservazione e alla cancellazione dei Dati personali del Titolare in possesso o controllo.

Diritti degli interessati

- assisterà il Titolare del trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati; qualora gli interessati esercitino tale diritto presso il Responsabile o sub-Responsabile del trattamento, quest'ultimo è tenuto ad inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze al Titolare del Trattamento, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti, solo per i trattamenti in carico a RTI.

Data Breach

- Ai sensi dell'art. 33 del Regolamento UE, il RTI informa immediatamente 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 quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il RTI si impegna a supportare il Titolare nell'ambito di tale attività.
- Il RTI deve avvisare immediatamente e senza ingiustificato ritardo il Titolare 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 il Titolare nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del contratto.

Revisione

- Testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Utilizzo di risorse informatiche del Titolare

Nel caso in cui il RTI utilizzi i sistemi informatici del Titolare mediante postazioni di lavoro dello stesso, per il trattamento dei dati le seguenti misure di sicurezza sono da considerarsi obbligatorie:

- Utilizzare sistemi e le ulteriori risorse informatiche del Titolare con gli scopi e obiettivi oggetto del contratto, evitando un trattamento dei dati non consentito o non conforme alle finalità del servizio erogato;
- Non effettuare trattamenti che possano in qualunque modo impattare sulla riservatezza, disponibilità o confidenzialità dei dati del Titolare;
- Non esportare su chiavetta o altro supporto dati prelevati dai sistemi, dai data base o dai server del Titolare;

- Non installare applicativi o tool web sulle postazioni lavorative del Titolare salvo espressa autorizzazione di quest'ultimo;
- Non modificare in nessun modo le configurazioni delle risorse informatiche a meno di approvazione esplicita del Titolare;
- Durante l'attività svolta nella sede del Titolare, applicare le regole di sicurezza fisica e comportamentali stabilite del Titolare.

Utilizzo di risorse informatiche proprie

Nel caso in cui il RTI utilizzi le proprie risorse informatiche per il trattamento dei dati del Titolare le seguenti misure di sicurezza sono da considerarsi obbligatorie:

Distruzione/Cancellazione dei dati

- Prevedere la cancellazione di file elettronici e/o dispositivi contenenti dati altamente confidenziali o riservati in modo sicuro dopo che i dati non sono più necessari e che, nel caso in cui i dispositivi non siano più utilizzati, siano distrutti con metodologie di distruzione sicura;
- Prevedere un processo che stabilisca come i dati del Titolare saranno conservati o rimossi. Nel processo sono specificati durata di conservazione, metodologia di conservazione e metodo di eliminazione. In particolare:
  - Documentare i requisiti di conservazione dei dati del Titolare, se presenti, come e dove verranno conservati i dati dopo la fine del progetto.
  - Documentare il processo mediante il quale i dati del Titolare che non devono essere conservati verranno rimossi. Indicare la frequenza di tali rimozioni, strumenti utilizzati, persona responsabile ecc."

Crittografia e conservazione dei dati

- Applicare adeguati meccanismi di cifratura a livello di hard disk in linea con gli standard di sicurezza internazionali su tutte le postazioni di lavoro utilizzate;
- Utilizzare adeguati meccanismi di crittografia a livello di file in linea con gli standard di sicurezza internazionali per conservare dati altamente confidenziali del Titolare fuori dagli ambienti applicativi;
- Utilizzare soltanto dispositivi mobili che siano stati adeguatamente crittografati secondo gli standard di sicurezza internazionali per conservare in modo temporaneo i dati del titolare e verificare che i dati sono eliminati definitivamente quando non più necessari.

Sicurezza fisica delle dotazioni informatiche

- Implementare controlli di sicurezza per garantire la sicurezza delle dotazioni informatiche dei dipendenti per evitare accessi non autorizzati, manomissioni e/o furti dei dispositivi utilizzati quali, ad esempio, il collegamento del notebook al cavo di blocco (cavo kensington), il blocco del desktop quando ci si allontana dalla postazione o l'utilizzo di strumenti di privacy filter.

Dispositivi e strumenti di lavoro

- Garantire l'uso di meccanismi di crittografia degli hard disk su tutte le postazioni utilizzate;
- Utilizzare solo dispositivi mobili crittografati per conservare in modo temporaneo e/o definitivo i dati del Titolare;
- Proibire l'uso di tool web, non autorizzati dal Titolare, per conservare dati del Titolare;
- Proibire la pubblicazione o archiviazione dei dati riservati del Titolare inclusi ID, PW, indirizzo IP e dati personali o aziendali su server di terze parti, non autorizzati dal Titolare;

- Vietare l'utilizzo di strumenti o siti di archiviazione o di backup di proprietà personale o di terze parti che non sono forniti o autorizzati dal titolare per archiviare i dati dei clienti;
- Prevedere per le postazioni di lavoro un anti-malware aggiornato.

Back-up

- Vietare l'utilizzo di strumenti o siti di archiviazione o di backup di proprietà personale o di terze parti che non sono forniti o autorizzati dal Titolare per archiviare i dati dei Titolari;
- Garantire che tutti i dati di progetto (software, documenti, ecc.) siano sottoposti al processo di backup attraverso una soluzione approvata dal Titolare, e siano accessibili solo alle persone autorizzate.

Riutilizzo delle informazioni o di deliverable.

- Identificare un singolo punto di contatto per la condivisione o la rimozione di file e informazioni al di fuori del team del Titolare o dell'ambiente del Titolare (prodotti di lavoro in uscita). Le richieste di informazioni (interne o client) devono essere inoltrate attraverso il processo appropriato.

Trasmissione digitale dei dati

- Utilizzare adeguati meccanismi di crittografia in linea con gli standard di sicurezza internazionali per trasmettere i dati del Titolare via internet;
- Utilizzare adeguati meccanismi di crittografia a livello di file, in linea con gli standard di sicurezza internazionali, per conservare dati altamente confidenziali del Titolare fuori dagli ambienti applicativi;
- Utilizzare solo account e-mail del Titolare per la trasmissione di dati altamente confidenziali;
- Utilizzare collegamenti sicuri per condividere file, o SFTP, o mantenere all'interno del dominio di posta elettronica del client. La predisposizione dell'infrastruttura necessaria per la condivisione è a cura del Titolare. Non utilizzare OneDrive for Business per condividere i dati del Titolare.

Gestione degli accessi degli utenti

- A ciascun individuo sono assegnate ID e password univoche. I singoli ID utente non devono essere condivisi;
- Se risulta necessario l'utilizzo di Application ID, a ciascuna applicazione deve essere associato un Application ID univoco e gli utenti individuali, compreso il system administrator, non devono utilizzare il Application ID per accedere ai sistemi.

Requisiti di sicurezza generali

I seguenti requisiti di sicurezza sono da considerarsi sempre applicabili:

Notifica Incidente

- Il RTI provvede a comunicare al Titolare, tempestivamente e in ogni caso senza ingiustificato ritardo, che si è verificata una violazione dei dati da quando il RTI, o un suo terzo autorizzato, ne ha avuto conoscenza o ha avuto elementi per sospettarne la sussistenza.

Formazione

- I componenti del team di lavoro hanno effettuato corsi di formazione in ambito di protezione dei dati del Titolare prima di iniziare a lavorare in tale ambito;

- Si impegnerà a elaborare e tenere i registri, nel rispetto delle tempistiche concordate, per assicurare che tutto il Personale impegnato sul progetto sia in regola con i presenti requisiti di sicurezza dalla fase di roll-on fino a quella di roll-off del progetto.

Distruzione copie cartacee

- Prevedere la distruzione delle copie cartacee contenenti i dati del Titolare in modo non reversibile;
- Per le Fotocopiatrici sono suggerite due modalità alterative fra loro:
    - Configurare le fotocopiatrici che possono essere utilizzate per i dati altamente riservati o limitati in modo da eliminare i dati in modo sicuro dopo ogni utilizzo. La configurazione è a cura del Titolare presso le sedi dello stesso o del RTI per dispostivi collocati presso le sedi del RTI.
    - In alternativa è necessario avere cura di spegnere le fotocopiatrici per eliminare i contenuti della cache (condizione valida se la memoria cache della fotocopiatrice non è di tipo persistente)

Change Management

- Mantenere un inventario aggiornato del tipo di dato del Titolare contenente una classificazione delle informazioni in base a criteri di confidenzialità e prevedere idoneo periodo di data retention concordato con il Titolare, trascorso il quale i dati devono essere cancellati.

Principio del minimo privilegio

- Applicare il concetto di "segregation of duties" in modo che nessuna persona abbia la possibilità di svolgere attività che potrebbero creare un conflitto di sicurezza (ad esempio: sviluppatore / revisore, sviluppatore / tester).

Gestione accessi degli amministratori

- Mantenere aggiornato l'elenco degli amministratori e relativi privilegi individuali all'interno di applicazioni o set di dati. Il responsabile della sicurezza delle informazioni (o designato) gestirà il registro di controllo degli accessi, rivedendoli non meno di ogni trimestre per confermare l'accuratezza;
- Notificare per scritto la nomina ad amministratore in modo che l'individuo sia a conoscenza del livello di accesso privilegiato richiesto come amministratore.

Sviluppo sicuro e revisione del codice

- Il codice è sviluppato secondo i requisiti OWASP e prima di essere rilasciato in ambiente di produzione o verso il Titolare è stato oggetto di un processo di code review dal punto di vista della sicurezza.

Roma,04/04/2019

Per l'Amministrazione

_____

Letto, approvato e sottoscritto digitalmente

_____

Il Fornitore