Comune di Gallarate
Protocollo Generale
N. 0002392 del 12/01/2023
Class: 04/10

0007730724

GRUPPO FINMATICA

Alla c.a. Dott. Colombo Michele
Spett.le
COMUNE DI GALLARATE
Via Verdi 2
21013 Gallarate

Bologna, 10/01/2023

Prot.: ADS_PV23 1616 23200048

OGGETTO: Attività di aggiornamento in sicurezza di applicazioni SAAS già erogate in ADSCloud

Come da accordi si fornisce offerta per quanto indicato in oggetto. Si evidenzia che la presente offerta attua, all'interno della Missione 1 Componente 1 del PNRR, finanziato dall'Unione europea nel contesto dell'iniziativa NextGenerationEU, l'Investimento 1.2 "ABILITAZIONE AL CLOUD PER LE PA LOCALI". L'investimento è collegato all'obbligo, introdotto dall'art. 35 del D.L. 76/2020, per la PA di migrare i propri CED verso ambienti cloud.

ADS automated data systems S.p.A.

Guido Montemartini

ADS
ADS Automated Data Systems S.p.A. - Via della Liberazione 15 - 40128 Bologna
Tel +39 (0)51 6307411 Fax +39 (0)51 6307498 web www.ads.it e-mail marketing@ads.it

Ad integrazione del servizio SAAS già in uso presso ADSCloud, si propongono una serie di attività di **aggiornamento delle infrastrutture** finalizzate ad **incrementare il livello di sicurezza delle applicazioni oltre ai livelli standard definiti dalla normativa AGID**.

Il percorso di ADS per la qualificazione

La missione di **ADS** è quella di progettare e realizzare soluzioni d'avanguardia che permettano di semplificare i processi della Pubblica Amministrazione e la condivisione delle informazioni mettendo a fattor comune conoscenze e capacità allo scopo di introdurre innovazioni radicali per la creazione di valore.

Nel 2018 ADS ha intrapreso il percorso per qualificare nel Catalogo Cloud di AgID i propri servizi cloud. Tale percorso si è sviluppato nelle seguenti tappe:

- a dicembre 2018 ADS ha ottenuto la certificazione ISO 27001 del sistema di gestione della sicurezza delle informazioni per l'erogazione di Servizi PaaSCloud (Platform as a Service) con l'utilizzo delle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019;
- a gennaio 2019, una volta ottenuta la certificazione ISO 27001, ADS si è qualificata quale Cloud Service Provider (CSP) di Tipo B sulla base dei requisiti richiesti dalla Circolare AgID n. 2 del 2018;
- a febbraio 2019 ADS ha qualificato quale soluzione erogabile in SaaS la suite **Smart*Gov** sulla base dei requisiti richiesti dalla Circolare AgID n. 3 del 2018.

Lo schema seguente riepiloga le principali fasi del processo

Lo standard **ISO 27001** costituisce, a tutt'oggi, il principale standard internazionale che certifica la capacità di garantire la sicurezza del patrimonio informativo. I Data Center ADS certificati ISO 27001, ubicati in località distanti tra loro oltre 100 km per garantire la continuità di servizio, sono situati all'interno di strutture altamente industrializzate, dotate dei più moderni sistemi, impianti e risorse professionali; sono predisposti per una connessione ad Internet attraverso linee multiple per una capacità complessiva di oltre 10 Gbit/s e sono dotati di sistemi di condizionamento, gruppi di continuità, generatori elettrici, sistemi antincendio, antiallagamento ed antintrusione e monitoraggio attivo 24x7.

In termini applicativi, la qualificazione SaaS della suite **Smart*Gov** nel Catalogo Cloud di AgID ha richiesto**,** tra gli altri prerequisiti, **l'applicazione della metodologia OWASP a garanzia dei livelli di sicurezza forniti delle funzioni software**. Nel contesto del processo di qualificazione, abbiamo aderito alla CSA (Cloud Security Alliance), sul sito della quale è consultabile la documentazione completa, all'indirizzo https://cloudsecurityalliance.org/star/registry/ads-automated-data-system-s-p-a

Prima di ogni rilascio di nuove versioni vengono effettuati test di sicurezza in parte tramite l'utilizzo di tool automatici ed in parte da personale adeguatamente formato sul tema sicurezza e sulla ricerca delle vulnerabilità. I test unitari sono lanciati sia dagli sviluppatori (prima di rilasciare modifiche al codice) sia in automatico ad ogni modifica del codice sorgente. Il sistema di Continuous Integration, ad ogni modifica del codice, verifica la corretta compilazione, permettendo di riscontrare eventuali errori di compilazione, errori di mancato rilascio di parti di codice o di modifiche delle dipendenze da librerie interne e di terze parti.

I test di sicurezza sono eseguiti utilizzando i sistemi messi a disposizione dal Open Web Application Security Project (**OWASP**), sia per l'analisi statica del codice con il controllo delle vulnerabilità delle librerie utilizzate, sia per l'analisi dinamica del flusso dei dati sulle richieste http.

Il rilascio di una versione nuova del prodotto può essere effettuato solo dopo aver superato con esito positivo tutti i test.

Attività di aggiornamento delle infrastrutture

Migrazione Virtual Machine da Storage SAS a Storage full

L'attività ha l'obiettivo di migliorare le performance della soluzione applicativa in SAAS

Gestione allegati documentale su server dedicato VMJDOC

L'attività ha l'obiettivo di migliorare il processo di backup e aumentare la consistenza dei dati contenuti su File System e Database

Attivazione snapshot storage per tutte le Virtual machine su storage SSD

L'attività ha come obiettivo l'attivazione dello snapshot storage per tutte le Virtual machine

Attivazione snapshot storage del server VMJDOC su storage NFS

L'attività ha come obiettivo l'attivazione snapshot storage per il server VMJDOC

Attivazione Replica della Virtual machine dedicata al DATABASE sul sito di Disaster Recovery

L'attività ha l'obiettivo di attivare il Disaster recovery per la componente dati presente all'interno del Database

Attivazione Replica della Virtual machine VMJDOC sul sito di Disaster Recovery

L'attività ha l'obiettivo di attivare il Disaster recovery per la componente dati del documentale presente su file system

Attivazione Replica della Virtual machine applicative sul sito di Disaster Recovery

L'attività ha l'obiettivo di attivare il Disaster recovery per la componente applicativa

Integrazione servizi SAAS

NETOBK Servizio di offline backup - Storage Snapshot

Come forma ulteriore di protezione delle VM e dei relativi dati utilizziamo le funzionalità di snapshot dei nostri storage. Questo consente di mantenere sul sito di produzione una copia ulteriore del dato non direttamente raggiungibile né in alcun modo attaccabile; tale "immagine" può tuttavia essere utilizzata per ripristini sia granulari che completi dell'ambiente in produzione.

NETDRINF – Servizio di Disaster recovery INFRASTRUTTURE applicative

La soluzione comporta la replcia delle virtual machine presso il sito alternativo, permettendo un recovery time piu' veloce. Il sito dispone di hardware e connettività già funzionante ma su scala inferiore rispetto al sito principale o ad un site alternativo sempre disponibile. Il backup avviene in modalità elettronica mediante collegamenti fra i siti tenuto dimensionati tenendo conto della tipologia, quantità e periodicità dei dati da backup-are

- RPO - Recovery Point Objective 24 ore (tempo massimo di delay tra l'ultima copia e il fault dei sistemi)
- RTO - Recovery Time Objective 1 ora (tempo necessario per il ripristino dei sistemi)

Attività di aggiornamento in sicurezza delle infrastrutture applicative

Upgrade dei sistemi operativi Linux ad Oracle Linux 8.5

L'attività integrativa rispetto alla migrazione dei sistemi in modalità Lift & shift consiste nella reinstallazione di tutti i server con sistema operativo Oracle Linux 8.5 con l'abilitazione della mantenance per l'applicazione controllata delle patch di sicurezza.

Upgrade degli application server Tomcat alla versione 9 (*)

L'attività integrativa rispetto alla migrazione dei sistemi in modalità Lift & shift consiste nella reinstallazione di tutti i contesti Tomcat in versione 9 con Security Support attivo.

(*) solo per i contesti applicativi compatibili

Upgrade/Migrazione database Oracle alla versione 19(**)

L'attività integrativa rispetto alla migrazione dei sistemi in modalità Lift & shift consiste nella migrazione o upgrade del database Oracle alla versione 19

(**) solo quando tutte le applicazioni risulteranno compatibili

Attivazione protocollo HTTPS

La soluzione applicativa al termine della configurazione utilizzerà esclusivamente **connessioni sicure**; la comunicazione applicativa, sia se esposta verso Internet ma anche se utilizzata attraverso un canale VPN avverrà mediante cifratura TLS ed il servizio di Presentazione esporrà l'applicativo web tramite protocollo HTTPS.

Attivazione autenticazione LDAP o LDAPS

Per ottemperare alla normativa GDPR si rende necessaria una normalizzazione degli utenti utilizzati per l'accesso alle procedure che prevede la creazione di utenti nominali e l'eliminazione di ogni utenza generica ad uso di più persone. Nell'ambito di questo processo si propone l'attivazione dell'autenticazione integrata con il Dominio AD in uso.
Per raggiungere l'obiettivo il piano di lavoro proposto prevede:

- Test query LDAP sui domini configurati
- Creazione gruppo utenti con caratteristiche d'accesso integrate al dominio LDAP
- Inserimento di uno user applicativo nel gruppo utenti LDAP
- Test di accesso applicativo con la password di dominio
- Estrazione profili utenti configurati all'interno del sistema AD4 su foglio di lavoro EXCEL
  - ✓ A carico del CLIENTE - Associazione all'interno del foglio di lavoro delle utenze di dominio a ciascun utente applicativo
  - ✓ A carico del CLIENTE - Identificazione delle utenze applicative condivise non associabili ad un singolo user di dominio
  - ✓ A carico del CLIENTE - Inserimento nel foglio di lavoro EXCEL delle utenze di dominio assenti in AD4 per la loro creazione in automatico.
  - ✓ A carico del CLIENTE - Inserimento nel foglio di lavoro EXCEL delle utenze da revocare.
- Creazione utenze nominative per manutenzione e test software ad uso Service Desk Fornitore.
  - ✓ A carico del CLIENTE - Caricamento e normalizzazione con utenti campione degli utenti in AD4 previa comunicazione all'utenza.
  - ✓ A carico del CLIENTE - Caricamento e normalizzazione contemporanea di tutti gli utenti in AD4 . i rapporti e le comunicazioni con l'utente finale sono a carico del Cliente"Assegnazione ruoli e competenze ai nuovi utenti creati in AD4.

PREREQUISITO: utenza abilitata a query LDAP sul dominio senza scadenza della password.

Supporto alla compilazione allegato DNSH (schede 6 e/o 8)

Prerequisito per il completamento della procedura per accedere ai fondi del Piano PNRR bando Cloud è la compilazione dell'allegato DNSH. Verrà fornito il supporto per la compilazione dei moduli relativi ai servizi forniti da Ads e contestualmente consegnate le certificazioni necessarie per giustificare le dichiarazioni di conformità fornite.

Compilazione verbale di collaudo e fine attività

Al termine delle attività verrà rilascio un verbale di collaudo e fine attività contenente la descrizione della configurazione dell'infrastruttura ad inizio progetto quella rilasciata in produzione.

Prezzo dei servizi offerti

N.	Modulo	Descrizione	Prezzo
1	SY_CON	Attività di aggiornamento in sicurezza delle infrastrutture • Migrazione Virtual Machine da Storage SAS a Storage full • Gestione allegati documentale su server dedicato VMJDOC • Attivazione snapshot storage per tutte le Virtual machine su storage SSD • Attivazione snapshot storage del server VMJDOC su storage NFS • Attivazione Replica della Virtual machine dedicata al DATABASE sul sito di Disaster Recovery • Attivazione Replica della Virtual machine VMJDOC sul sito di Disaster Recovery • Attivazione Replica della Virtual machine applicative sul sito di Disaster Recovery	**1.120**
2	NET_THST	Integrazione servizi SAAS fino al **31/12/2024**	**1.660**
3	SY_CON	Attività di aggiornamento in sicurezza delle infrastrutture applicative: • Upgrade dei sistemi operativi Linux ad Oracle Linux 8.5	**3.220**

		• Upgrade/Migrazione database Oracle alla versione 19(*) • Upgrade degli application server Tomcat alla versione 9(**) • Attivazione protocollo HTTPS • Attivazione autenticazione LDAP o LDAPS • Supporto alla compilazione allegato DNSH (In caso di adesione al finanziamento PNRR - schede 6 e/o 8) • Compilazione verbale di collaudo e fine attività (*) solo per i contesti applicativi compatibili (**) solo quando tutte le applicazioni risulteranno compatibili	

TOTALE ATTIVITA' UNA TANTUM E INTEGRAZIONE SERVIZIO SAAS FINO AL 31/12/2024 € 6.000

Condizioni di fornitura

Tempi di consegna e validità dell'offerta

La presente offerta ha una validità di 60 giorni.
Per l'accettazione dell'offerta è condizione necessaria che la presente ritorni alla Società debitamente sottoscritta in tutte le sue parti ed allegati entro il periodo di validità. In mancanza, qualora dovesse pervenire l'accettazione della presente con diverse modalità, le clausole della presente offerta e di tutti i contratti allegati si intenderanno tutte, nessuna esclusa, concordate ed accettate dal Cliente.

Tempi di consegna

I tempi di consegna per la realizzazione di quanto offerto verranno con Voi in seguito concordati; si ipotizza comunque la consegna entro 150 giorni dall'ordine.
Nel caso di personalizzazioni del software applicativo o di ritardi nella consegna dell'hardware o del software di base da parte del fornitore originale verranno comunicati tempestivamente eventuali differimenti nei termini sopra indicati.

Pagamenti e Fatturazione

Il pagamento dovrà essere effettuato entro "30 giorni data fattura" dalle singole fatture, che verranno emesse alla data di consegna delle singole personalizzazioni. In caso di ritardati pagamenti verranno applicate le disposizioni di cui al D.Lgs. 231/2002 e successive modificazioni.

Responsabilità

La Società non assume alcuna obbligazione oltre a quelle previste dal presente contratto e, salvo il caso di dolo o colpa grave, non assume alcuna responsabilità per i danni di qualsiasi natura comunque sofferti dal Cliente in relazione all'oggetto del presente contratto o alle prestazioni previste nello stesso. La Responsabilità della Società non può essere superiore al valore della fase cui si riferisce.

Disposizioni generali

Contestazioni. Qualunque contestazione sulle prestazioni effettuate dalla Società deve, a pena di nullità, essere effettuata in forma scritta entro dieci giorni dalla consegna del prodotto o dalla erogazione del servizio.
Estensioni. Tutto quanto qui convenuto si applica, in quanto compatibile, anche alle prestazioni extracontrattuali.
Adempimenti in tema di tracciabilità finanziaria - Legge 136/2010. La Società si obbliga ad osservare le disposizioni contenute nell'art. 3 della legge n. 136/2010 e successive modifiche o integrazioni in materia di tracciabilità dei flussi finanziari. La Società si obbliga altresì ad inserire nei contratti sottoscritti con i sub appaltatori e i sub contraenti apposita clausola con la quale ciascuna delle parti si assume gli obblighi previsti dall'art. 3 della Legge n. 136/2010 e successive modifiche e integrazioni. La Società si impegna a dare immediata comunicazione al Cliente della notizia dell'inadempimento della propria controparte (sub appaltatore - sub contraente) agli obblighi di tracciabilità finanziaria. Ai sensi dell'art. 3 comma 9 bis della Legge n. 136/2010, il presente contratto si risolve automaticamente di diritto nel caso di violazione degli obblighi in materia di tracciabilità.
Costi della sicurezza. Il prezzo della fornitura è comprensivo dei costi della sicurezza afferenti all'esercizio dell'attività svolta dall'impresa. I costi che la Società sostiene per gli adempimenti di cui al DLgs. .81/2008 e succ. modificazioni corrispondono allo 0,5% del valore del corrispettivo.

Privacy e Protezione dei Dati Personali

Le parti potranno, nel corso dello svolgimento del contratto, avere accesso a dati e ad informazioni ad esso connessi e si impegnano ad utilizzarli esclusivamente ai fini del raggiungimento degli obiettivi dell'incarico, nonché a mantenere riservate le informazioni di cui potranno venire a conoscenza nel rispetto della vigente normativa sulla privacy (D.Lgs. 196/03) e del regolamento Europeo in materia di protezione dei dati n. 679/2016 (GDPR).
Il Cliente con la sottoscrizione del presente offerta presta il consenso al trattamento dei dati da parte della Società, ai sensi delle vigenti disposizioni in materia di trattamento dei dati personali, per le finalità connesse all'esecuzione del presente contratto.
Nel rispetto del GDPR si allegano l'informativa sul trattamento dei dati personali connesso all'esecuzione del contratto e l'"Accordo per il trattamento dei dati ai sensi del Reg. UE 679/2016" . Il Cliente si impegna a fornire alla Società i dati di sua competenza, utilizzando l'apposita sezione dell'allegato Accordo e restituendone copia.

Subappalto

La Società, nell'ambito dell'intera fornitura, può eventualmente subappaltare a terzi o a società del Gruppo Finmatica, i servizi indicati in offerta, nel rispetto dell'art. 105 del D.lgs. 50/2016 e s.m.i.
Rimane comunque invariata la responsabilità del fornitore contraente, il quale continuerà a rispondere di tutti gli obblighi contrattuali

Competenza

In caso di controversia sarà competente esclusivamente il Foro di Bologna.

Rinvii

Per tutto quanto non previsto e non in opposizione si rimanda quale parte integrante all'offerta, alle norme e condizioni generali del Contratto di Licenza d'uso del software applicativo allegato .

Firma del Cliente

_____

Firma delLa Società

_____

CLAUSOLE DI SPECIFICA APPROVAZIONE

Agli effetti degli articoli 1341 e 1342 Codice Civile sono specificatamente approvate le clausole di cui agli articoli:
Modalità di Accettazione della fornitura – Responsabilità – Contestazioni – Foro Competente Privacy e Protezione dei Dati e Subappalto.

Bologna, lì_____

Firma del Cliente per accettazione

_____

Informativa sul trattamento dei dati personali connesso all'esecuzione del contratto

Nel rispetto dell'art. 13 del Regolamento UE 679/2016 – Regolamento Generale Protezione Dati (GDPR), i dati personali forniti dal Cliente all'inizio e nel corso del rapporto, saranno trattati dalla nostra Società quale titolare, per la conclusione ed esecuzione del Contratto e per l'adempimento dei connessi obblighi normativi, amministrativi, contabili e fiscali.
La Società indicata nel presente contratto, è titolare del trattamento unitamente alle altre Società del gruppo Finmatica (che costituiscono un «gruppo imprenditoriale» ai sensi dell'art. 4, paragrafo 19 del GDPR, per cui hanno deliberato di definire congiuntamente le finalità ed i mezzi del trattamento dei dati al fine di procedere in qualità di "Contitolari del trattamento" ex art. 26 del Reg. UE 679/2016 alla piena attuazione del Regolamento Europeo).

Il conferimento dei dati personali (contatti) da parte del Cliente è necessario per le predette finalità o comunque obbligatorio per l'adempimento degli obblighi contrattuali e normativi. Il mancato rilascio, anche in parte, di questi dati personali potrebbe precludere l'instaurazione del rapporto e renderne non possibile la gestione.

Per le predette finalità i dati saranno trattati con procedure prevalentemente informatizzate e potranno essere conosciuti da nostri dipendenti, collaboratori ed organismi di vigilanza autorizzati al trattamento e/o da società, che in qualità di responsabili del trattamento, possono svolgere alcune attività tecniche ed organizzative per nostro conto, quali società di servizi amministrativi, contabili e fiscali, società di servizi informatici. I dati del Cliente potranno essere inoltre comunicati alle seguenti categorie di soggetti: - amministrazioni pubbliche (Agenzia Entrate per l'adempimento di obblighi normativi; - società del gruppo a fini amministrativi interni e/o di gestione del contratto.

I dati raccolti saranno conservati per tutta la durata del Contratto ed, in genere, per 10 anni dalla data della sua cessazione.

Il GDPR garantisce alla persona fisica a cui si riferiscono i dati (c.d. Interessato) il diritto di accedere in ogni momento ai dati che la riguardano ed ottenerne copia, di rettificarli ed integrarli se inesatti o incompleti, di cancellarli o limitarne il trattamento ove ne ricorrano i presupposti, di opporsi al loro trattamento per motivi legati alla situazione particolare dell'Interessato e/o comunque per fini di marketing diretto, di chiedere la portabilità dei dati forniti ove trattati in modo automatizzato sulla base del Suo consenso o per l'esecuzione del contratto. L'Interessato ha altresì diritto di revocare il consenso, ove richiesto, senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca. Resta infine fermo il diritto dell'Interessato di rivolgersi al Garante Privacy, anche attraverso la presentazione di un reclamo, ove ritenuto necessario, per la tutela dei Suoi dati personali e dei Suoi diritti.

Per qualsiasi questione attinente al trattamento dei dati personali l'Interessato può rivolgersi alla nostra Società, quale contitolare del trattamento, oppure può contattare il nostro Responsabile della protezione dei dati (RPD/DPO), ai seguenti recapiti:

Responsabile del trattamento:

Legale Rappresentante p.t.
Via della Liberazione, 15 – 40128 Bologna
Tel. 0516307411
email privacy@ads.it

Responsabile della protezione dei dati (RPD/DPO):

Roberto Labanti
Via della Liberazione, 15 – 40128 Bologna
Tel. 0516307411
Cell. 3294715617
email: dpo@finmatica.it

Consenso per finalità di marketing

1) SISTEMA DI OPT-IN EX ART. 130, COMMI 1 E 2, CODICE PRIVACY (DIRETTIVA 2002/58/CE)

Previo consenso del Cliente, i dati che lo riguardano potranno essere inoltre trattati dalla nostra Società per finalità di commercializzazione diretta (c.d. direct marketing) quali l'invio di materiale pubblicitario, vendita diretta, compimento di ricerche di mercato o comunicazioni commerciali per posta, telefono, sistemi automatizzati di chiamata, fax, e-mail, sms, mms, relativi a prodotti e servizi della nostra Società e di altre società operanti nel settore dell'Information Communication Technology. Per queste finalità, il rilascio dei dati e del consenso è comunque facoltativo e non ha conseguenze sulla conclusione ed esecuzione del Contratto. In ogni momento, il Cliente ha comunque il diritto a revocare il consenso eventualmente prestato.

☐ Acconsento/iamo al trattamento dei dati da parte della Vostra Società a fini di marketing diretto.

2) SISTEMA DI OPT-OUT EX ART. 130, COMMA 4, CODICE PRIVACY (VALIDO SOLO PER E-MAIL)

L'indirizzo di posta elettronica fornito dal Cliente per la gestione del Contratto sarà inoltre utilizzato dalla nostra Società per l'invio di comunicazioni a fini di commercializzazione diretta di prodotti o servizi analoghi a quelli oggetto del Contratto cui è riferita la presente informativa. Il Cliente può opporsi in ogni momento alla ricezioni di tali comunicazioni barrando l'apposita casella in calce al presente Contratto o scrivendo alla Società, ai recapiti sopra riportati.

☐ Non voglio/iamo ricevere comunicazioni e-mail a fini di marketing diretto di prodotti o servizi della Vostra Società.

Accordo per il trattamento dei dati ai sensi del Reg. UE 679/2016 (GDPR)

Obblighi assunti dalla Società quale Responsabile del trattamento dei dati personali

In base a quanto previsto dall'art. 8 delle Norme e Condizioni Generali comuni a tutti i servizi, di cui il presente documento fa parte integrante, qui di seguito vengono indicati gli obblighi assunti dalla Società, quale Responsabile del trattamento, nella persona del suo Legale Rappresentante p.t., nello svolgimento per conto del Cliente, quale Titolare, delle attività di trattamento dei dati personali connesse alla fornitura dei Servizi di cui al Contratto.

In particolare, la Società, in qualità di Responsabile del trattamento, si impegna a:

I. trattare i dati personali sulla base delle documentate istruzioni fornite dal Cliente quale Titolare;

II. adottare adeguate misure per la sicurezza dei dati personali previste dal GDPR, indicate dal Titolare e/o individuate ai sensi del Contratto o dalla legge, vigilando sulla applicazione delle stesse, in modo da ridurre al minimo i rischi di violazione dei dati medesimi;

III. individuare le persone autorizzate al trattamento dei dati personali che operano sotto la propria autorità e garantire che le persone autorizzate assumano idonei obblighi di riservatezza di tali dati, fornendo loro adeguate istruzioni per lo svolgimento delle attività di trattamento e verificandone l'osservanza;

IV. "conservare direttamente e specificatamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema" esclusivamente per quanto necessario per lo svolgimento di quanto previsto dal Contratto e all'attività di verifica almeno annuale dell'operato di questi amministratori di sistema "in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza, riguardanti i trattamenti dei dati personali, previste dalle norme vigenti" (come previsto dal Provvedimento del Garante sugli "amministratori di sistema" pubblicato in G.U. n. 300 del 24 dicembre 2008 e dalla sua modifica in base al provvedimento del 25 giugno 2009);

V. assistere il Cliente nel garantire il rispetto, per quanto di relativa competenza, degli obblighi in tema di sicurezza, notifica all'autorità di eventuali violazioni di dati personali e, se del caso, loro comunicazione agli interessati, nonché di valutazione d'impatto sulla protezione dati ed eventuale consultazione preventiva, ai sensi degli articoli da 32 a 36 del GDPR, tenendo conto delle documentate istruzioni impartite dal Titolare in relazione all'adempimento dei suddetti obblighi, nonché della natura del trattamento e delle informazioni a disposizione dello stesso Responsabile;

VI. comunicare al Titolare per iscritto, senza indebito ritardo, eventuali violazioni di sicurezza che riguardino i dati personali trattati ai fini della fornitura dei Servizi oggetto del Contratto;

VII. informare tempestivamente il Cliente in caso di ricevimento di richieste di informazioni o documenti, accertamenti ed ispezioni, da parte del Garante per la protezione dei dati personali, quale autorità competente di controllo, o di altre autorità giudiziarie o di polizia giudiziaria, ove attinenti al trattamento dei dati personali connesso alla fornitura dei Servizi oggetto del Contratto, e collaborare con il Titolare alla predisposizione dei correlati riscontri, atti, documenti o comunicazioni;

VIII. cancellare o restituire al Cliente, su richiesta di quest'ultimo, tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che la vigente normativa europea o nazionale preveda la conservazione dei dati da parte del Responsabile che, in tal caso, ne darà contestuale attestazione al Titolare.

La Società dichiara e garantisce che eventuali ulteriori 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 dalla Società nei confronti del Cliente.

Al Cliente è riservata la facoltà di richiedere le modificazioni e/o integrazioni degli obblighi previsti in capo alla Società quale Responsabile del trattamento che si rendano necessarie a seguito dell'eventuale entrata in vigore di nuove disposizioni di legge, di regolamento ovvero di provvedimenti adottati da autorità amministrative o giudiziali in materia di tutela dei dati personali.

Di seguito i dati di contatto del Responsabile del trattamento:
email: privacy@finmatica.it
Telefono: 0516307411

RPD (DPO) della Società

La Società, congiuntamente alle altre società del proprio gruppo aziende (gruppo Finmatica) si è avvalsa della facoltà prevista dall'art. 37 punto 2 del GDPR per procedere alla nomina di un "Responsabile unico della protezione dei dati" (RPD oppure DPO).

L'esigenza di un RPD è sorta non solo per proteggere i trattamenti effettuati dalle aziende del gruppo in quanto contitolari ma soprattutto per quelli effettuati dalle singole aziende del gruppo in quanto responsabili.

Di seguito i dati di contatto del RDP (DPO) della Società:
nome: Roberto Labanti
email: dpo@finmatica.it
Cellulare: 3294715617
Telefono: 0516307411

Le misure tecniche e organizzative delle aziende del Gruppo Finmatica - SGSI

Al fine di recepire quanto previsto dal GDPR, la Società, congiuntamente alle altre aziende del gruppo Finmatica, ha adeguato la propria politica della sicurezza delle informazioni e i relativi obiettivi aggiornando il proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI), riferimento per tutte le procedure e le istruzioni inerenti alla sicurezza delle informazioni e alla protezione dei dati personali. Questa nuova versione del SGSI tende ad una maggiore conformità rispetto alla ISO/IEC 27001:2013.

Le misure tecniche e organizzative, "Privacy by design" e "Privacy by default"

Sono tante le misure che il titolare, in base al principio di "responsabilizzazione" ("accountability") previsto nell'art. 5 del Regolamento, deve mettere in atto. Fra queste, ci sono quelle previste dall'art. 24 secondo il quale il titolare del trattamento (quindi tutti gli Enti e le Aziende che gestiscono dati personali) deve mettere "in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento".
Fra le misure tecniche e organizzative che il titolare dei trattamenti deve mettere in atto ci sono quelle previste dall'art. 25 comma 1, cioè la "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita". In questo articolo c'è una premessa da tenere presente, cioè che il titolare dovrà attuare queste misure "tenendo conto dello stato dell'arte e dei costi di attuazione" oltre che del contesto (tipo di dati, finalità, ecc.). Quindi, la "Privacy by design" non ha delle regole precise ma è una progettazione per rispondere ai "principi di protezione dei dati".
Sempre nell'art. 25, il comma 2 prevede che "siano trattati, per impostazione predefinita, solo i dati personali necessari": anche la "Privacy by default" è possibile da una integrazione di misure tecniche ed organizzative.

La conformità del software al GDPR

Anche l'art. 32, "Sicurezza del trattamento", con la stessa premessa dell'art. 25 ("tenendo conto dello stato dell'arte e dei costi di attuazione"), non fornisce una lista precisa delle misure tecniche e organizzative adeguate ma solo delle indicazioni "tra le altre, se del caso": insomma si tratta di una lista aperta e non esaustiva, lontana dalla impostazione del "Disciplinare tecnico in materia di misure minime di sicurezza" dell'allegato B del D.Lgs. 196/2003.
Con queste premesse, una dichiarazione precisa per certificare la conformità di un software al GDPR non è possibile (mentre lo era rispetto al D.Lgs. 196/2003): ACCREDIA ha proposto uno schema di certificazione volontario per determinare la conformità al Regolamento (ISDP 10003:2015), ma ci sono due problemi: si tratta di uno schema che non certifica solo un prodotto software ma anche processi e servizi e, soprattutto, il Garante ha dichiarato che "a legislazione vigente non possono definirsi conformi agli artt. 42 e 43 del regolamento 2016/679, poiché devono ancora essere determinati i requisiti aggiuntivi ai fini dell'accreditamento degli organismi di certificazione e i criteri specifici di certificazione" .
Insomma, per poter effettuare una dichiarazione certa di conformità del software al GDPR, si dovranno attendere le indicazioni del Garante, che è "l'autorità di controllo competente" anche per le certificazioni, come previsto dall'art. 43 del Regolamento.

Contatti titolare e RPD (DPO) del Cliente per registro delle attività di trattamento della Società

Il Cliente, titolare del trattamento, fornisce i dati di contatto utili per il "registro delle attività del trattamento" che la Società, responsabile del trattamento ex art. 28 del GDPR, deve tenere secondo quanto previsto dall'art. 30 punto 2 del GDPR:

Titolare del trattamento:

nome e cognome : _____

email: _____

Telefono: _____

Responsabile della protezione dei dati (RPD oppure DPO) del Cliente:

nome e cognome: _____

email: _____

Telefono: _____