

CONTRATTO SPECIFICO PER SERVIZI DI TRAFFIC MANAGEMENT EROGATI IN MODALITA' SaaS

- Addendum informativo -

Tra

I&S Informatica e Servizi S.r.l. con sede legale in Via dei Solteri 74, 38121 Trento (TN), CF e PI 00665230223 – Reg. Imprese REA TN n. 0130099) e sede operativa nella stessa sede, in persona del suo legale rappresentante ing. Pier Luigi Fedrizzi CF FDRPLG49H09F837T (denominata anche I&S o **Fornitore**)

al fine di mettere a disposizione del "**Committente**" (denominato anche **Cliente**) un opportuno set informativo che consenta a quest'ultimo di usufruire della migliore esperienza possibile di servizio ed identificare prontamente le modalità di gestione di eventuali problematiche connesse direttamente o indirettamente ad esso oltre che esprimere il soddisfacimento dei requisiti richiesti da ACN per la qualifica dei propri servizi alla Pubblica Amministrazione in conformità con le linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019.

Quanto riportato all'interno del presente documento è da intendersi ad integrazione e migliore precisazione delle informazioni contenute nelle condizioni generali di contratto essendo un allegato allo stesso,

INFORMA

di quanto segue.

1) COLLOCAZIONE GEOGRAFICA E LUOGO DI CONSERVAZIONE DEI DATI (Rif. 6.1.3 ISO 27017 – A12.1 ISO 27018)

I&S Informatica e Servizi S.r.l. ha sede legale ed operativa in Trento (TN) Italy. L'infrastruttura informatica necessaria alla erogazione dei servizi di Bollettazione clienti (WOW/DBW), gestione flotta (LeOWeb), sportello on line (SOL), WebGIS (3wGIS) e dei relativi server dedicati è collocata presso:

- Fornitore qualificato e certificato ISO 27001 nella sede in Germania (DE) e Finlandia (FI), attraverso l'utilizzo della piattaforma IaaS.
- Fornitore qualificato ACN con dati localizzati in Italia, attraverso l'utilizzo di un'infrastruttura livello QI2 IaaS.

Dette infrastrutture tecnologiche virtuali sono nella disponibilità esclusiva del Committente, che ne gestisce la configurazione e l'erogazione del servizio. In ogni caso la conservazione dei dati avviene nell'ambito del territorio italiano ed europeo, ai fini della individuazione della legislazione applicabile in caso di controversia.

2) RUOLI E RESPONSABILITÀ (Rif. 6.1.1 della ISO 27017 e 6.1.1 ISO 27018)

I&S Informatica e Servizi S.r.l. ha provveduto ad identificare specifiche responsabilità per l'erogazione dei servizi Cloud tramite la documentazione dei sistemi di gestione ISO 9001 e ISO 27001 che sono a disposizione e documentati all'interno dell'organizzazione tramite opportuni organigrammi.

I riferimenti per contatti tecnici e commerciali relativi ai servizi cloud sono i seguenti:

Commerciale: ing. Daniele Dati
I&S Informatica e Servizi S.r.l. - Via dei Solteri 74 – 38121 Trento (TN)
Telefono: 0461 402122 - Fax: 0461 402114
eMail: commerciale@ies.it - PEC: informaticaeservizi@legalmail.it

Tecnico Security Manager: ing. Annelise Vulcan
I&S Informatica e Servizi S.r.l. - Via dei Solteri 74 – 38121 Trento (TN)
Telefono: 0461 402122 - Fax: 0461 402114
Piattaforma Ticket: <https://redmine.ies.it>
eMail di supporto Web comunicata al Project Manager.
Per problematiche relative alla sicurezza utilizzare eMail: security@ies.it

3) ATTIVAZIONE DEI SERVIZI (Rif. 6.1.1 della ISO 27017 e 6.1.1 ISO 27018)

I&S Informatica e Servizi S.r.l. è impegnata ad attivare tempestivamente i servizi richiesti dal Cliente al momento della sottoscrizione delle condizioni contrattuali, che riportano la tipologia di servizi abilitati sulla Piattaforma, trasmettendo tempestivamente al Cliente username e link per la generazione della password di accesso di cui al successivo punto 4 del

presente set informativo per la prima utenza detta "Amministrativa". Per la natura stessa dei servizi e grazie all'utilizzo della piattaforma SaaS il cliente può autonomamente attivare ulteriori utenti rispetto a quelli originariamente contrattualizzati direttamente dalla piattaforma, attraverso le credenziali di autenticazione di amministratore. Sono presenti opzioni ed servizi aggiuntivi che il cliente può sottoscrivere ed acquistare in aggiunta per il proprio servizio (es: Visure MCTC, Reportistica avanzata, Integrazione VMS e Active Directory, etc..) che dovranno essere richieste al commerciale di riferimento del Fornitore e che saranno attivate in backoffice dal Fornitore stesso.

Dove è previsto l'intervento in backoffice di I&S Informatica e Servizi S.r.l. la stessa è impegnata ad attivare le nuove risorse e servizi entro e non oltre 3 giorni lavorativi dalla richiesta, ovvero a riscontrare la richiesta del Cliente entro lo stesso termine in caso di insorgenza di problematiche o necessità di chiarimenti. Nessuna responsabilità potrà comunque essere ascritta al Fornitore per il caso di ritardo nell'attivazione del servizio; la richiesta di chiarimenti o la segnalazione di eventuali problematiche, da eseguire utilizzando la piattaforma di ticket precedentemente riportata, determina dal momento dell'invio la sospensione del termine di attivazione.

E' facoltà del Cliente chiedere a I&S Informatica e Servizi S.r.l., mediante comunicazione inviata tramite la piattaforma di ticketing o via e-mail, la messa a disposizione di risorse o servizi aggiuntivi rispetto a quelli già attivati. In tal caso alla richiesta inoltrata dal Cliente farà seguito da parte di I&S Informatica e Servizi S.r.l., di norme entro 3-5 giorni lavorativi dalla ricezione della richiesta, la redazione di un preventivo specifico in base alla disponibilità delle risorse o dei servizi richiesti. Il momento perfezionativo dell'accordo dove in questo caso intendersi identificato nella conferma da parte del Cliente dell'accettazione del preventivo ricevuto, da cui decorre anche il termine per l'attivazione delle risorse o dei servizi contrattualizzati previsto dal precedente capoverso.

4) CRITERI DI AUTENTICAZIONE (Rif. 9.2.1-9.2.2-9.2.3-9.2.4 della ISO 27017 e 9.2.1 – 9.4.2 ISO 27018)

All'attivazione del servizio I&S Informatica e Servizi S.r.l. fornisce al Cliente uno username (di norma corrispondente alla mail di contatto) ed una password per l'accesso "amministrativo" alla piattaforma.

La piattaforma al primo accesso obbliga l'utente alla variazione della password che è scelta sempre dagli utenti e non conosciuta dal Fornitore. Il Fornitore, su richiesta del Committente, può procedere all'attivazione della funzionalità 2FA.

L'amministratore dell'istanza sarà poi autonomo nella creazione degli ulteriori utenti, e relativa attribuzione di ruoli, e sarà sua cura comunicare agli utenti finali le relative credenziali che saranno comunque da cambiare al primo accesso della piattaforma.

Salva diversa e specifica pattuizione a richiesta del Cliente, la password inserita dovrà essere composta da almeno otto caratteri, comprendenti almeno un carattere speciale, una maiuscola.

L'onere di provvedere alla regolare modifica della password di accesso viene assunto dal cliente, il quale deciderà tempi e modalità per la scadenza delle password; lo stesso per la conservazione delle credenziali di accesso e della non divulgazione di esse anche ai fini della prevenzione di accessi non autorizzati. Fatto salvo quanto infra specificato per il caso di crittografia dei dati, I&S Informatica e Servizi S.r.l. si impegna a prestare assistenza al Cliente – ove necessario – per eventuali modifiche delle credenziali di accesso ovvero recupero delle stesse in caso di smarrimento. Eventuali richieste di supporto tecnico o reset della password dovranno essere inoltrate all'indirizzo eMail come riportato sul sito web. A tutela della sicurezza dei dati e delle infrastrutture, I&S Informatica e Servizi S.r.l. accetterà le richieste solo se provenienti dal referente dell'istanza del servizio o autorità riconosciuta (es: resp. Acquisti o responsabile dei servizi IT) e si riserva di richiedere l'esibizione di dati che consentano l'identificazione del richiedente o comunque la conferma della provenienza della richiesta dall'avente diritto, ed in ogni caso di verificare con qualunque mezzo l'effettivo potere di quest'ultimo.

Le piattaforme permettono una profilazione granulare delle utenze che sono configurabili dall'utente amministratore dell'istanza Cloud tramite la gestione di Ruoli organizzativi. Alle utenze, sempre l'amministratore dell'istanza Cloud, associa successivamente i Ruoli organizzativi assegnati.

I sistemi di sicurezza implementati per l'accesso alle piattaforme Cloud prevedono un filtraggio del traffico che risulta abilitato per i soli collegamenti provenienti dal territorio italiano. I&S Informatica e Servizi S.r.l. si riserva di valutare ulteriori configurazioni o sviluppi tecnologici per aumentare il livello di verifica e controllo degli accessi.

Tramite l'analisi dei log, disponibili anche per l'amministratore dell'istanza, è possibile visualizzare gli accessi effettuati dove risultano anche gli accessi negati permettendo una analisi di potenziali account compromessi.

Non risultano attivi controlli ed automatismi che prevedono la disabilitazione o la cancellazione delle utenze in quanto visto la natura dei servizi, anche investigativi, sarebbe controproducente per gli utilizzatori. E' pertanto responsabilità del cliente la gestione delle utenze compresa l'abilitazione, la disabilitazione e la variazione dei ruoli autorizzativi degli account in sua gestione.

All'interno delle piattaforme dei servizi cloud erogati da I&S Informatica e Servizi S.r.l. sono presenti interfacciamenti con banche dati di servizio e di settore di volta in volta configurate (es: Google per le mappe, sistemi contabili esterni, servizi e provider per invio di notifiche a grandi linee) che prevedono l'inserimento delle credenziali di tali servizi all'interno delle istanze dei servizi cloud. Tali credenziali risultano integralmente di proprietà del cliente e da lui gestite ed immesse nelle relative schermate di configurazione delle sue istanze. I&S Informatica e Servizi S.r.l. è responsabile della corretta archiviazione e protezione ma non sarà responsabile di un uso scorretto da parte del cliente delle sue credenziali.

5) CRITTOGRAFIA (Rif. 10.1 della ISO 27017 e 10.1 ISO 27018)

Salvo diversa ed esplicita richiesta del Cliente, I&S Informatica e Servizi S.r.l. non effettua alcuna attività di crittografia dei dischi o dei dati collocati dai Clienti all'interno dei servizi a loro assegnati.

È attiva la crittografia sul canale di comunicazione con certificati gestiti da I&S Informatica e Servizi S.r.l. per l'accesso al web server ed all'istanza del cliente. È inoltre attivo un canale crittografato su VPN con certificati autogenerati relativo al collegamento con i server dei servizi Cloud atti a ricevere dati e informazioni per le successive elaborazioni.

E' comunque facoltà del Cliente richiedere all'atto della stipula del contratto -ovvero successivamente ad esso mediante accordo aggiuntivo da sancire in forma scritta - la collaborazione da parte di I&S Informatica e Servizi S.r.l. per l'implementazione di procedure di crittografia dei dati, internamente alla macchina virtuale del cliente ma tale soluzione prevede come pre-requisito la gestione Single-Tenant dell'istanza del cliente che porterà ad una definizione di un contratto specifico con il cliente al fine di determinare i relativi costi previsti.

La gestione delle chiavi di crittografia relative ai servizi sopra descritti saranno gestite da I&S Informatica e Servizi S.r.l. in quanto necessarie per l'erogazione dei servizi stessi. Per la gestione di tali chiavi sono presenti specifiche procedure di sicurezza delle informazioni all'interno delle certificazioni ISO 27001 e ISO 9001 gestite da I&S Informatica e Servizi S.r.l.

Dovrà inoltre considerarsi a carico esclusivo del cliente la verifica della compliance della tipologia di crittografia sviluppata o richiesta alla normativa nazionale di riferimento per competenza o materia, dipendendo tali informazioni dalla tipologia di attività svolta dal cliente, dalla natura dei dati trattati e dalle finalità sottese al trattamento dei medesimi.

6) MODIFICHE AL SERVIZIO (Rif. 12.1.2 della ISO 27017)

Per garantire la migliore esperienza dei servizi offerti e consentire al Cliente il monitoraggio delle condizioni di erogazione dei servizi, I&S Informatica e Servizi S.r.l. è impegnata a rendere nota la versione applicativa dei servizi Cloud erogati direttamente in interfaccia utilizzata dal cliente.

Il versionamento applicativo viene diffuso, in base alle necessità, con comunicazione mirata ai clienti via eMail o Redmine in cui si dettagliano gli aggiornamenti e/o le modifiche dell'infrastruttura ovvero della piattaforma che siano tali da non comportare alcun prevedibile effetto negativo relativamente all'erogazione del servizio. La pubblicazione di dette informazioni, poiché relative a interventi che non costituiscono prevedibilmente alcun rischio per il servizio o per il cliente, costituisce principio di trasparenza da parte del fornitore, pur in assenza di ogni obbligo contrattuale al riguardo.

I&S Informatica e Servizi S.r.l. è altresì impegnata a comunicare al cliente, mediante trasmissione di comunicazione diretta, l'effettuazione di modifiche hardware o software che abbiano il prevedibile effetto di incidere negativamente sulla disponibilità e qualità dei servizi e sulla sicurezza delle informazioni e dei dati del Cliente. Fatto salvo il caso di causa sopravvenuta ed imprevedibile o forza maggiore, tutte le modifiche programmate all'infrastruttura che si rendano necessarie per la prosecuzione o il miglioramento del servizio e che abbiano il prevedibile effetto di incidere negativamente sulla qualità dei servizi, saranno comunicate al Cliente e con lo stesso cliente viene definita la data di aggiornamento dei servizi. All'atto della comunicazione saranno indicati da I&S Informatica e Servizi S.r.l. il tipo di intervento che sarà effettuato, la prevedibile durata di esso, i prevedibili effetti sul servizio e/o eventuali, prevedibili, situazioni di rischio per i dati del Cliente, se del caso gli eventuali accorgimenti da assumere a cura del Cliente per la migliore tutela dei dati e ripresa della piena funzionalità del servizio. Nel tempo di preavviso stabilito con il Cliente potrà sempre richiedere chiarimenti e/o precisazioni mediante i contatti riportati sopra o comunque tramite il sistema di Ticketing Redmine oppure l'eMail del supporto tecnico specifico per ogni applicativo (vedi punto 2).

Nel caso di modifiche che dovessero rendersi necessarie per effetto di atti, fatti o comunque eventi non prevedibili, tali da determinare l'urgenza di provvedere, I&S Informatica e Servizi S.r.l. è impegnata a svolgere tutte le attività di modifica con le modalità tecniche che siano ritenute le migliori disponibili per la garanzia della qualità del servizio e la sicurezza dei dati di proprietà del Cliente; per quanto possibile I&S Informatica e Servizi S.r.l. si impegna a comunicare al Cliente l'avvio delle operazioni e lo stato di avanzamento delle stesse.

Al termine di ogni modifica, sia essa pianificata e previamente comunicata ovvero improvvisa e quindi strettamente necessaria, I&S Informatica e Servizi S.r.l. provvederà all'invio ai propri Clienti di comunicazione attestante l'avvenuto completamento delle operazioni ed il relativo esito.

7) BACKUP (Rif. 12.3.1 della ISO 27017 e 12.3.1 ISO 27018)

I&S Informatica e Servizi S.r.l. gestisce le policy di backup dei dati dei servizi Cloud erogati ai clienti. I backup sono eseguiti secondo le seguenti policy di default:

- Tutti i dati sono oggetto di backup a livello di VM con cadenza quotidiana incrementale a fronte di un backup completo a cadenza settimanale. La retention di backup dei dati è pertanto di 7 giorni.
- I backup sono effettuati tramite l'applicativo CommVault con memorizzazione su istanza indipendente del servizio IaaS erogata direttamente dal Datacenter in modo da garantire una completa separazione dei dati rispetto alle macchine gestite da I&S Informatica e Servizi S.r.l. I backup sono crittografati come previsto dal servizio fornito.
- I backup vedono una verifica periodica su base semestrale che viene verificata direttamente da I&S Informatica e Servizi S.r.l. e documentata all'interno dei processi dei sistemi di gestione. Il tempo di ripristino delle macchine è inferiore alle 8 ore.
- La localizzazione dei backup è: Datacenter ISO 27001 in Finlandia, oppure Datacenter in Italia qualificato ACN Q12.

È altresì facoltà del Cliente, all'atto della stipula del contratto o successivamente ad essa, chiedere la predisposizione a cura di I&S Informatica e Servizi S.r.l. di servizi di backup ulteriori rispetto a quelli disponibili all'interno della piattaforma, sia interni che esterni ad essa. In tal caso, seguirà all'eventuale richiesta del Cliente la predisposizione da parte di I&S Informatica e Servizi S.r.l. di un preventivo come previsto al punto 2 del presente set informativo, secondo capoverso, e con gli effetti ivi indicati.

8) SINCRONIZZAZIONE OROLOGIO (Rif. 12.4.4 della ISO 27017)

Per la determinazione dell'orario dei servizi cloud offerti, I&S Informatica e Servizi S.r.l. utilizza di norma l'ora fornita da INRIM - Istituto Nazionale di Ricerca Metrologica. Non è possibile accettare richieste di personalizzazione delle configurazioni su specifica del cliente in quanto tali configurazioni sono applicate all'intera infrastruttura gestita da I&S Informatica e Servizi S.r.l.

9) INFORMAZIONI RELATIVE ALLA SICUREZZA NELLE FASI OPERATIVE E DI SVILUPPO (Rif. 14.2.1 della ISO 27017 – 13.2.1 della ISO 27018)

I&S Informatica e Servizi S.r.l. è impegnata a mettere a conoscenza del Cliente la tipologia dei servizi di sicurezza utilizzati per la tutela dei dati da questo trattati attraverso l'infrastruttura in cloud, ovvero a concordare con il cliente – dietro pagamento di un corrispettivo per la personalizzazione – l'installazione, l'implementazione o comunque l'utilizzo di livelli di sicurezza. I&S Informatica e Servizi S.r.l. in particolare si impegna a mettere a disposizione unicamente le conoscenze e gli elementi che sono indispensabili al Cliente per ottenere la migliore esperienza d'uso dei servizi contrattualizzati, rimanendo peraltro facoltà di I&S Informatica e Servizi S.r.l. di non divulgare elementi anche dei sistemi di sicurezza che per tipologia o per caratteristiche oggettive possano essere suscettibili di un uso malevolo da parte di eventuali terzi soggetti, con rischio per la sicurezza dei dati e/o per l'infrastruttura. Salvo sia diversamente disposto nel Contratto o in eventuali pattuizioni aggiuntive, I&S Informatica e Servizi S.r.l. utilizza di norma sistemi di sicurezza della rete (ex. Firewall, segregazione delle reti tramite vLan, policy di zero trust), sicurezza dei sistemi (ex. monitoraggio dell'uso delle risorse) e sicurezza gestionale (ex. applicazione di patch correttive e di sicurezza) per la protezione dell'infrastruttura da utilizzi impropri o prevedibili rischi di sicurezza, essendo riconducibili a I&S Informatica e Servizi S.r.l. le responsabilità relative al funzionamento della piattaforma SaaS e PaaS, con garanzia della disponibilità dei servizi al Cliente con le caratteristiche e le risorse contrattualizzate.

Nel caso di sviluppo di nuove procedure o aggiornamento degli applicativi propri e/o di terze parti, I&S Informatica e Servizi S.r.l. è impegnata a rispettare una politica di sviluppo sicuro mediante effettuazione dei test di funzionamento in ambienti di sviluppo separati rispetto a quelli in cui viene garantita l'operatività del servizio, al fine della individuazione di eventuali bug o malfunzionamenti prima della messa in esercizio degli applicativi nella versione aggiornata, il tutto in osservanza degli standard

internazionali in materia di procedure di sviluppo sicuro. Nel caso di necessità di provvedere ad attività di sviluppo e/o aggiornamento delle componenti di terze parti come ad esempio l'aggiornamento delle librerie.

Periodicamente è prevista una scansione con tool di analisi delle vulnerabilità al fine di effettuare i dovuti aggiornamenti dell'infrastruttura a fronte delle vulnerabilità identificate.

Negli ambienti di sviluppo utilizzati per i test I&S Informatica e Servizi S.r.l. è impegnata a non utilizzare dati del Cliente, che devono intendersi unicamente residenti sugli ambienti operativi allo stesso concessi e nella disponibilità esclusiva di quest'ultimo. Qualora, al fine di verificare nel contraddittorio eventuali problematiche riscontrate o malfunzionamenti, dovesse essere il Cliente a richiedere a I&S Informatica e Servizi S.r.l. delle procedure di testing aggiuntive e specifiche in ambiente protetto, con utilizzo di dati riconducibili alla propria disponibilità, I&S Informatica e Servizi S.r.l. si rende disponibile a mettere a disposizione gli ambienti di sviluppo e ad assistere il Cliente nei test richiesti, con successiva cancellazione di tutti i dati del Cliente eventualmente utilizzati -su richiesta e consenso di quest'ultimo- per le attività rese necessarie.

Al fine di facilitare la generazione di dati per gli ambienti di Test, Sviluppo e Demo I&S Informatica e Servizi S.r.l. ha creato un generatore randomico di eventi / passaggi di automezzi al fine di facilitare la creazione di dati che siano sempre indipendenti dai dati di produzione del cliente.

Salvo esplicita richiesta del Cliente, I&S Informatica e Servizi S.r.l. non utilizza per il trasferimento dei dati supporti fisici esterni, preferendo per ragioni di sicurezza e tracciabilità trasferimenti esclusivamente virtuali. In caso di utilizzo di supporti fisici a richiesta del Cliente saranno concordate con quest'ultimo le tipologie di supporto, le modalità di utilizzo degli stessi e gli elementi atti a garantire la sicurezza dei dati del Cliente e dell'infrastruttura di proprietà di I&S Informatica e Servizi S.r.l. utilizzata per l'erogazione dei servizi cloud. Tale attività prevedrà un progetto specifico da contrattualizzare specificatamente con il cliente.

10) PEER CLOUD SERVICES e SUBFORNITORI (Rif. 15.1 della ISO 27017)

Nell'ambito dei servizi proposti, come dichiarato precedentemente, I&S Informatica e Servizi S.r.l. utilizza come richiesto da ACN provider qualificati di Infrastruttura e Servizi IaaS. La scelta di I&S Informatica e Servizi S.r.l. è stata per un provider con dati localizzati in Italia qualificato ACN QI2.

Se non richiesta la qualificazione ACN sarà possibile utilizzare un Datacenter certificati ISO 27001, dislocato in Germania e in Finlandia.

Per l'erogazione dei servizi cloud I&S Informatica e Servizi S.r.l. non si avvale dell'intervento di subfornitori che effettuino trattamento di dati, che quindi vengono conservati all'interno del perimetro dell'infrastruttura tecnologica direttamente riconducibile alla proprietà ed al controllo di I&S Informatica e Servizi S.r.l.;

Sono previsti interfacciamenti dei servizi cloud offerti sia con provider di settore (per es. Enti locali, società multiservizi, protezione civile, etc.) sia con provider tecnici (server di invio eMail, social network del cliente, etc..) che risultano però sotto la gestione e la configurazione dell'istanza a cura del cliente e pertanto da lui scelti ed impostati. Sarà pertanto cura del cliente e del suo processo di trattamento dei dati la gestione di tali fornitori.

11) RACCOLTA DELLE EVIDENZE (Rif. 16.1 della ISO 27017 - 16.1, A10.1 della ISO 27018)

Qualora si evidenzino elementi che consentano di ritenere fondato il timore di sottoposizione dei dati a rischi o incidenti, I&S Informatica e Servizi S.r.l. è impegnata a mettere a disposizione del Cliente che lo richieda la propria collaborazione per l'accertamento dell'esistenza o meno della vulnerabilità e, in caso affermativo, della sua causa.

Ricordando che il contratto del servizio cloud SaaS è corredato da un incarico dato a I&S Informatica e Servizi S.r.l. di responsabile esterno al trattamento dei dati fornito dal titolare del trattamento dei dati rappresentato dal cliente; I&S Informatica e Servizi S.r.l. è responsabile di attuare gli accordi privacy definiti in tale accordo.

Dove un cliente possa anche solo sospettare di una vulnerabilità o una perdita di riservatezza, integrità e disponibilità di dati ed informazioni dei servizi cloud provvederà a contattare il supporto tecnico ai riferimenti sopra riportati. Sarà cura di I&S Informatica e Servizi S.r.l. prendere in carico tali ticket con una coda di priorità atta a garantire una risposta congrua con i tempi previsti legislativamente per le comunicazioni agli enti preposti che dovrà effettuare il cliente (es: 72 ore nel caso di Data Breach).

Si ricorda che in ottica *private by design* sono già presenti nelle piattaforme funzionalità opzionali ed attivabili atte a garantire che le immagini e le informazioni estratte dalle piattaforme cloud siano "etichettate" con dati relativi a chi ha effettuato l'estrazione. Log applicativi sono comunque disponibili in merito alle estrazioni effettuate e sono sia disponibili direttamente al cliente all'interno dell'istanza per gli utenti abilitati sia fornibili in formati ulteriori su specifica richiesta del cliente.

Nel caso in cui sia I&S Informatica e Servizi S.r.l. ad avere certezza o anche solo sospetto della verifica di un incidente che possa avere un impatto sulla riservatezza, integrità o disponibilità dei dati, ovvero in caso di segnalazione da parte di Autorità o gruppi specialistici di security di attività impattanti, I&S Informatica e Servizi S.r.l. è impegnata a comunicare tali circostanze al Cliente non appena avutane la conoscenza e comunque entro quaranta ore dalla conoscenza avutane, mediante invio di mail all'indirizzo di contatto indicato nel contratto; il Cliente è tenuto a riscontrare la comunicazione entro e non oltre trentadue ore dal suo invio da parte di I&S Informatica e Servizi S.r.l. al fine dell'assunzione congiunta delle iniziative ritenute più opportune per la tutela dei dati presenti e delle infrastrutture; in caso di mancata risposta da parte del Cliente quest'ultimo sarà ritenuto esclusivo responsabile in caso di compromissione o perdita dei dati dallo stesso gestiti.

Qualora a seguito di segnalazione di Autorità o gruppi specialistici di security, ovvero anche mediante analisi interna, I&S Informatica e Servizi S.r.l. abbia evidenza dell'utilizzo degli spazi cloud concessi al Cliente con finalità malevole e/ comunque pericolose per altri utenti o sistemi, il fornitore di servizi si intenderà autorizzato a svolgere ogni più opportuno intervento per impedire l'uso malevolo a tutela della comunità degli utenti – siano essi interni alla piattaforma o anche esterni – dovendosi intendere compresa anche, quale *extrema ratio* – la temporanea sospensione del servizio che può avvenire in due modalità:

- Sospensione del servizio web di accesso alle piattaforme dei servizi cloud ma lasciando attivi i servizi di ricezione dati del back-end
- Sospensione completa del servizio.

In entrambi i casi sarà data tempestiva comunicazione al Cliente attraverso l'indirizzo mail di contatto.

12) PROTEZIONE DEI DATI (Rif. 18.1 della ISO 27017 – A2, A3, A6, A11.1 della ISO 27018)

Per quanto concerne la protezione dei dati, I&S Informatica e Servizi S.r.l. è impegnata a rispettare la legislazione italiana in materia, ivi espressamente comprese le norme derivanti dai regolamenti europei e/o direttive direttamente applicabili, tra le quali il Reg. UE n. 679/2016 "GDPR", consentendo ai Clienti l'esercizio dei relativi diritti e con le garanzie di protezione ivi previste come meglio indicate nella informativa privacy che I&S Informatica e Servizi S.r.l. mette a disposizione dei propri clienti sul sito aziendale. In tutti i casi I&S Informatica e Servizi S.r.l. si impegna a garantire, ove più elevati, gli standard per la sicurezza dei dati previsti da ACN – Agenzia per la Cybersecurity Nazionale e le best practices di volta in volta indicate dal CSIRT Italiano. Nell'ambito dell'attività aziendale tutto il personale coinvolto nelle attività è vincolato alla riservatezza con riferimento a tutte le informazioni apprese o trattate nell'esercizio delle proprie mansioni, come previsto dai regolamenti interni sia di Politica sicurezza dipendenti e Qualità sia degli incarichi al trattamento dei dati sottoscritto da tutto il personale addetto. A richiesta del Cliente, I&S Informatica e Servizi S.r.l. è disponibile a fornire al Cliente tutte le informazioni relative agli accorgimenti utilizzati per la tutela dei dati, previa sottoscrizione da parte del Cliente di impegno alla riservatezza e con la sola esclusione di elementi di dettaglio la cui divulgazione possa a sua volta costituire pericolo per la sicurezza dei dati o delle infrastrutture.

Salvo espressa e specifica autorizzazione del Cliente, da rilasciarsi alla stipula del contratto o mediante profilazione dell'utente nell'ambito della piattaforma, i dati di cui I&S Informatica e Servizi S.r.l. sia in possesso saranno utilizzati da quest'ultima ai fini del corretto e tempestivo adempimento delle obbligazioni contrattuali e della gestione tecnica ed amministrativa del rapporto inerente i servizi resi; I&S Informatica e Servizi S.r.l. è impegnata a verificare che anche i subfornitori e comunque tutti i soggetti che vengano a conoscenza di tali dati nell'ambito della normale gestione del contratto, ivi compresi a titolo esemplificativo ma non esaustivo professionisti esterni per la tenuta della contabilità o la gestione delle controversie, adottino le medesime limitazioni all'uso dei dati raccolti. I dati raccolti potranno essere utilizzati da I&S Informatica e Servizi S.r.l. per attività di marketing unicamente in presenza di espresso consenso del Cliente, da intendersi facoltativo e comunque non costituente condizione essenziale per l'erogazione dei servizi offerti.

Pur ricordando che la maggioranza degli utenti utilizzatori dei servizi cloud di I&S Informatica e Servizi S.r.l. sono Organi di Polizia e che essi stessi utilizzano le informazioni a scopo anche investigativo in qualità di autorità giudiziarie, nel caso in cui I&S Informatica e Servizi S.r.l. sia entrato in contatto con ulteriori autorità giudiziarie non clienti, I&S Informatica e Servizi S.r.l. è impegnata a verificare l'esistenza di un titolo idoneo e, alternativamente, (i) l'avvenuta notifica al Cliente dell'atto che legittimi l'accesso dell'Autorità ai dati, alla loro estrazione o sequestro per l'esercizio del diritto di difesa ove previsto ovvero (ii) che sussista una espressa e motivata richiesta dell'Autorità Giudiziaria di accesso senza evidenza al Cliente nell'ambito di atti di indagine coperti da riservatezza. In ogni caso I&S Informatica e Servizi S.r.l. è impegnata a prestare collaborazione con l'Autorità

Giudiziaria o mandataria di essa ai fini della prevenzione della commissione o perpetuazione di reati informatici ed all'identificazione delle responsabilità in caso di loro commissione; in considerazione di quanto precede, previa esibizione di titolo idoneo, I&S Informatica e Servizi S.r.l. è impegnata a collaborare con l'Autorità richiedente nello svolgimento delle attività di indagine limitatamente ai dati e/o comunque alle informazioni espressamente richieste o comunque rientranti nei limiti della delega di indagine conferita agli operanti. In tal caso I&S Informatica e Servizi S.r.l. osserva il più assoluto riserbo sulle circostanze apprese in occasione della collaborazione con l'Autorità inquirente anche nei confronti del Cliente, ove questo non sia stato già destinatario di atti dell'Autorità a seguito di disclosure degli atti di indagine.

Tutte le richieste di informazioni relative al trattamento dei dati e/o agli elementi di sicurezza utilizzati per la loro conservazione possono essere inoltrate dal Cliente all'indirizzo mail privacy@ies.it da intendersi quale punto di contatto del titolare del trattamento del dato. Le informazioni relative agli elementi di sicurezza utilizzati per la conservazione dei dati saranno comunicate unicamente laddove la conoscenza di essi da parte dei richiedenti non determini l'insorgenza di rischi per la detenzione e la sicurezza dei dati medesimi.

13) CONSERVAZIONE DEI LOG E DERIVED DATA (Rif. 12.4, 7.2.2, 8.1.1 della ISO 27017 – 12.4.1 della ISO 27018)

I&S Informatica e Servizi S.r.l. detiene direttamente informazioni dei LOG relativi alle piattaforme e alle macchine virtuali delle istanze dei servizi dei clienti e dei dati da esse derivati (Backup, agenti installati sui server, etc..) essendo gli stessi gestiti direttamente ed unicamente da I&S Informatica e Servizi S.r.l.

I log applicativi sono comunque disponibili anche per il Cliente all'interno delle piattaforme dei servizi cloud per gli utenti che ne hanno le relative abilitazioni, in quanto consultabili all'interno della propria istanza e saranno conservati da I&S Informatica e Servizi S.r.l. per un tempo conforme alla normativa applicabile (180 giorni). Si ricorda che i tempi di conservazione di altri elementi quali foto, passaggi e dati delle piattaforme sono di 7 giorni come impostazione di default a meno di richieste scritte inviate al support da parte del contatto autorizzato del cliente.

Qualora il Cliente avesse necessità di acquisire i log detenuti da I&S Informatica e Servizi S.r.l. e non disponibili al Cliente (ex. log relativi alla infrastruttura e/o di piattaforma) I&S Informatica e Servizi S.r.l. fornisce un servizio di assistenza dedicata per fornire i log richiesti in quanto è necessario una valutazione più approfondita al fine di depurare i log da eventuali informazioni di altri clienti (ambienti multi tenant) così come per applicare eventuali requisiti da stabilire con il cliente (Es: Marcatura temporale, firma digitale, etc..). Tali richieste saranno effettuate a fronte di un accordo contrattuale aggiuntivo.

Al termine del rapporto contrattuale, e fatti salvi i diritti previsti per il Cliente dal GDPR, I&S Informatica e Servizi S.r.l. è impegnata a mantenere i requisiti definiti nel punto 15.

14) VERIFICA DEGLI STANDARD DI SICUREZZA E AUDIT (Rif. 14.1, 18.2.1 della ISO 27017 – 18.2.1 della ISO 27018)

I&S Informatica e Servizi S.r.l., al fine di fornire evidenza della propria attenzione al mantenimento di elevati standard per la tutela dei dati e/o comunque per la sicurezza delle informazioni di proprietà e/o comunque nella disponibilità del Cliente, si impegna a sottoporre regolarmente le proprie procedure ad enti di certificazione indipendenti di parte terza, pubblicando sul sito internet www.ies.it il certificato conseguito, con indicazione degli enti certificatori, della data di rilascio della certificazione e della relativa validità ai fini del successivo rinnovo.

Qualora uno o più Clienti dovessero richiedere di effettuare audit di parte seconda, I&S Informatica e Servizi S.r.l. mette a disposizione del Cliente che ne faccia motivata richiesta una o più unità di personale per l'assistenza al Cliente nel corso dell'audit, a fronte del pagamento da parte di quest'ultimo – nel cui esclusivo interesse l'audit deve intendersi effettuato – di un corrispettivo orario per ciascuna unità di personale a disposizione pari ad euro 60,00 (sessanta/00) per ciascuna ora o frazione di ora. Rimane comunque la facoltà per I&S Informatica e Servizi S.r.l., a proprio giudizio insindacabile, di negare la fornitura di dati o elementi ovvero l'accesso ai luoghi di detenzione dei dati o di funzionamento delle infrastrutture tecnologiche qualora la divulgazione di essi o le conoscenze acquisite con l'accesso agli spazi possano determinare condizioni di pericolo per la sicurezza dei dati (del datacenter o di altri clienti dell'infrastruttura) o delle infrastrutture. In ogni caso, in occasione di eventuali audit di parte seconda il Cliente ed eventuali suoi delegati o incaricati dovranno previamente sottoscrivere un accordo di riservatezza relativo a tutte le informazioni e le conoscenze che dovessero apprendere nell'ambito dell'audit, di qualunque natura o specie, con impegno di questi ultimi sia a non utilizzarle direttamente nell'ambito della propria attività sia a non divulgarle né consentirne la divulgazione a terze parti. La sottoscrizione dell'accordo di riservatezza costituisce condizione essenziale per l'avvio delle procedure di audit da parte del Cliente o di suoi delegati/incaricati.

15) RIMOZIONE DEI DATI IN CASO DI CESSAZIONE DEL RAPPORTO (Rif. CLD 8.1.5 della ISO 27017 – A10.3 della ISO 27018)

Al termine del rapporto contrattuale per l'utilizzo dei servizi cloud erogati, I&S Informatica e Servizi S.r.l. consente ai Clienti una proroga dell'accessibilità della piattaforma per un periodo di 15 (quindici) giorni successivi alla scadenza del contratto, con limitazione delle potenzialità e dei servizi, al solo fine di consentire al Cliente di procedere all'esportazione e cancellazione di tutti i dati in qualunque forma presenti sulla piattaforma a sé riconducibili. La cancellazione dei dati dovrà essere effettuata a cura e spese del Cliente mediante accesso autonomo al suo ambiente e prevedendo una cancellazione sicura secondo le sue procedure organizzative. Al termine del processo il Cliente è tenuto a comunicare a I&S Informatica e Servizi S.r.l. l'avvenuto completamento dell'operazione, per la disabilitazione dell'utenza e la cancellazione dell'istanza del cliente dalla piattaforma o dai server. I&S Informatica e Servizi S.r.l. non sarà in alcun modo responsabile della perdita di eventuali dati del Cliente ancora presenti sull'infrastruttura successivamente alla comunicazione di avvenuto completamento delle operazioni di asportazione e cancellazione dei dati.

In caso di mancata comunicazione da parte del Cliente dell'avvenuta esportazione e cancellazione dei dati presenti sulla piattaforma, infruttuosamente decorsi i 15 giorni di cui al punto precedente I&S Informatica e Servizi S.r.l. procederà alla disabilitazione della possibilità di accesso del Cliente alla piattaforma. I dati eventualmente ancora presenti saranno mantenuti nella disponibilità a richiesta del Cliente per ulteriori 30 (trenta) giorni, decorsi i quali (ovvero allo scadere del quarantacinquesimo giorno successivo alla scadenza o risoluzione del contratto per una delle cause previste nel Contratto) I&S Informatica e Servizi S.r.l. procederà alla cancellazione di tutti i dati, delle macchine virtuali, dei backup collegati e alla rimozione dell'istanza del cliente dalle piattaforme e dai server. Decorso il termine così indicato, nessuna responsabilità potrà essere ascritta a I&S Informatica e Servizi S.r.l. per l'eventuale perdita dei dati ancora presenti, che devono intendersi oggetto di abbandono da parte dell'avente diritto ed oggetto di una presunzione assoluta di non unicità, stante il tempo infruttuosamente trascorso per l'eventuale salvataggio all'esterno della piattaforma.

16) RESPONSABILITA' IN CAPO AL CLIENTE (Rif. CLD 8.1.5 della ISO 27017 – A10.3 della ISO 27018)

Pur garantendo la sicurezza e la protezione dei dati attraverso pratiche certificate, i servizi SaaS di I&S Informatica e Servizi S.r.l. richiedono alcune responsabilità in capo al cliente per un utilizzo sicuro ed efficiente. Queste includono:

- gestione degli accessi e delle autenticazioni: il cliente è responsabile della gestione delle credenziali dei propri utenti e dell'implementazione di policy di accesso sicuro, inclusa l'abilitazione dell'autenticazione multi-fattore (MFA) per gli account con accesso privilegiato, ove applicabile;
- monitoraggio dell'utilizzo del servizio: è responsabilità del cliente verificare che le modalità d'uso del servizio SaaS rispecchino i requisiti operativi aziendali e che la capacità di servizio soddisfi le proprie esigenze;
- sicurezza delle informazioni e formazione del personale: il cliente deve assicurarsi che il proprio personale riceva un'adeguata formazione sui rischi associati all'uso di servizi cloud, promuovendo consapevolezza sui temi di sicurezza informatica e sugli standard operativi necessari per mantenere sicuro l'ambiente di lavoro;
- gestione della conformità e dei requisiti di sicurezza: anche se la gestione di backup e configurazioni dei servizi cloud sottostanti non è direttamente gestita dal cliente, lo stesso deve segnalare eventuali necessità aggiuntive o particolari, non indicate in questo documento, necessarie per adattarsi alle politiche aziendali interne, in modo da permettere ad I&S Informatica e Servizi S.r.l. di analizzare la casistica e di informarlo sulle possibilità di implementazione;
- gestione delle vulnerabilità e segnalazione di incidenti: il cliente è responsabile di segnalare prontamente qualsiasi attività sospetta, potenziali vulnerabilità o incidente di sicurezza rilevato, comunicando tramite i canali di supporto, in modo da permettere ad I&S Informatica e Servizi S.r.l. di intervenire rapidamente per mitigare eventuali rischi