All. A)

CAPITOLATO SPECIALE DESCRITTIVO E PRESTAZIONALE PER L'AFFIDAMENTO DEL SERVIZIO DI TESORERIA

Progetto del Servizio, come previsto dall'art. 23 del D.Lgs. 50/2016 Codice dei contratti commi 14 e 15

PARTE SECONDA

CAPITOLATO SPECIALE DESCRITTIVO E PRESTAZIONALE

INDICE

ART. 1
OGGETTO DELL'AFFIDAMENTO

Il Servizio di Tesoreria oggetto del presente affidamento si sostanzia nel complesso di operazioni legate alla gestione finanziaria dell'Azienda e finalizzate, in particolare, alla riscossione delle entrate ed al pagamento delle spese, nonché alla custodia di titoli e valori ed agli adempimenti connessi, previsti dalla legge, dallo statuto, dai regolamenti dell'Azienda o da norme pattizie.

Il Tesoriere dovrà in particolare provvedere:
a) alla riscossione di tutte le entrate dell'Azienda;
b) alla esecuzione di tutti i pagamenti dell'Azienda
c) ad accettare e custodire nelle sue casse, sotto la sua responsabilità, i depositi cauzionali fatti in relazione ad ammissione alle aste, o ad altro titolo.

Il Servizio dovrà essere svolto:
- nel pieno rispetto delle disposizioni normative vigenti in materia;
- nell'osservanza delle condizioni previste dal presente capitolato e nello schema di contratto approvato con Deliberazione del Consiglio di Amministrazione n. 2022/34 del 27/07/2022.
- in locali idonei, facilmente accessibili al pubblico e accessibili alle persone con disabilità
- in orari identici a quelli osservati per le operazioni bancarie, con rispetto dei limiti stabiliti dalle disposizioni contenute nel C.C.N.L. di categoria e nei relativi integrativi aziendali del Tesoriere.
- tutti gli sportelli del Tesoriere, almeno uno dei quali ubicato nel Comune di Reggio Emilia, dovranno operare in effettiva e completa circolarità per la registrazione delle operazioni di riscossione e pagamento con il rispetto della successione cronologica.

ART.2
MODALITA' DI EROGAZIONE – OBBLIGHI DELLE PARTI

Il Servizio dovrà essere reso sulla base delle indicazioni più sotto precisate, talune delle quali legate alla natura giuridica dell'Azienda (Azienda Servizi alla Persona) e derivanti dalla normativa e dalla disciplina contabile, anche regolamentare, ad essa applicabile
L'Azienda si obbliga ad informare il Tesoriere delle trasformazioni della propria natura giuridica nonché delle modifiche da essa derivanti relative al servizio di tesoreria , come sotto descritto, ed il Tesoriere si impegna ad accettarle ed ad adeguarvisi senza oneri.

L'Azienda opera con un sistema di contabilità economico-patrimoniale disciplinato sulla base dello Schema tipo di regolamento di contabilità per le Aziende pubbliche di servizi alla persona di cui alla Legge Regionale dell'Emilia Romagna n. 2 del 12.03.2003 approvato con Deliberazione della Giunta Regionale n. 279 del 12.03.2007 ed è informato alle disposizioni in materia di contabilità e bilancio di cui al Codice Civile.

Il Servizio richiede l'accensione di un Conto Corrente intestato all'Azienda.

A) ESERCIZIO FINANZIARIO
L'esercizio contabile dell'Azienda ha durata annuale con inizio il 1°gennaio e termine il 31 dicembre di ogni anno e tali date corrispondono agli effetti dei pagamenti e delle riscossioni, da operarsi in ciascun esercizio.

B) RISCOSSIONI
Il Tesoriere è tenuto ad incassare tutte le somme spettanti all'Azienda sotto qualsiasi titolo e causa, rilasciando, in suo luogo e vece, quietanza liberatoria.

Di norma le entrate saranno incassate dal Tesoriere in base ad ordini di riscossione (reversali) emesse dall'Azienda, numerati progressivamente sottoscritti digitalmente dal Direttore e dal Dirigente Area Risorse o loro sostituti. Per ogni somma incassata il Tesoriere rilascerà regolare quietanza numerata progressivamente, compilata con procedure e moduli meccanizzati e informatizzati. Annotazione di tali quietanze sarà annualmente raccolta in un elenco il cui totale dovrà corrispondere al totale delle entrate annotate dal Tesoriere nel giornale di cassa.

Il Tesoriere deve accettare, anche senza autorizzazione dell'Azienda, le somme che i terzi intendono versare, rilasciandone ricevuta contenente, oltre l'indicazione della causale del versamento, la clausola espressa "salvi i diritti dell'Azienda". Detti incassi, mancanti di ordinativi, rimarranno a disposizione dell'Azienda, alla quale il Tesoriere richiederà l'emissione dei relativi ordini di riscossione, che dovranno riportare la dicitura: "a copertura del sospeso n._____" rilevabile dal giornale di cassa fornito dal Tesoriere.
Le riscossioni fatte dal Tesoriere s'intendono pure e semplici, cioè senza l'onere "del non riscosso come riscosso" e senza l'obbligo di esecuzione contro i morosi da parte del Tesoriere, che non è tenuto ad intimare atti legali o richieste o ad impegnare le proprie responsabilità nelle riscossioni, rimanendo sempre a carico dell'Azienda ogni pratica legale ed amministrativa per ottenere l'incasso.
Il prelevamento dai conti correnti postali intestati all'Azienda è disposto esclusivamente dall'Azienda medesima, mediante emissione di ordinativo di incasso. L'accredito delle somme sul conto di Tesoreria sarà effettuato nello stesso giorno in cui il Tesoriere avrà la disponibilità della somma prelevata dal conto corrente postale.
Per quanto attiene la riscossione di rette, tariffe, contribuzioni varie, e canoni di locazione il tesoriere dovrà disporre di idonee procedure informatiche per la predisposizione dei titoli per il loro incasso in base alle modalità specificate al punto S del presente Articolo.
Il Tesoriere non applicherà alcuna commissione ai soggetti pagatori di rette, tariffe e contribuzioni varie, che effettueranno il pagamento agli sportelli.

C) PAGAMENTI
I pagamenti verranno effettuati esclusivamente in base ad ordini di pagamento (mandati) individuali o collettivi, emessi dall''Azienda, numerati progressivamente e sottoscritti digitalmente dal Direttore e dal Dirigente Area Risorse o loro sostituti.
I mandati devono contenere: il cognome, il nome, o la ragione sociale, la residenza del creditore, l'eventuale numero di c/c bancario o postale corredato dalle relative coordinate, la somma da pagare in lettere e in cifre, l'oggetto del pagamento e gli estremi dei documenti in base ai quali sono stati emessi.
Laddove ricorra il caso, ai fini della tracciabilità dei flussi finanziari e nel rispetto di quanto previsto dalla Legge 136/2010 art. 3 i mandati e gli strumenti di pagamento devono riportare, in relazione a ciascuna transazione il codice identificativo di gara (CIG) e, ove obbligatorio, il codice unico di progetto (CUP).

Il Tesoriere darà luogo, previo avviso da parte dell'Azienda, anche in mancanza del mandato e sotto comminatoria dell'indennità di mora, ai pagamenti che, per disposizione di legge o di contratto, facciano carico al Tesoriere stesso o siano da eseguirsi a scadenze improrogabili (rate mutui, canoni di utenze varie, stipendi, contributi previdenziali, premi assicurativi, imposte e tasse, pagamenti mediante addebito in conto o SEPA, ecc.). Inoltre in caso di necessità l'Azienda può autorizzare il tesoriere con apposita disposizione sottoscritta dai firmatari autorizzati a eseguire pagamenti urgenti ed indilazionabili, senza la contestuale emissione del mandato che sarà successivamente emesso a regolarizzazione.
L'Azienda si impegna ad emettere tempestivamente i mandati relativi ai suddetti pagamenti su comunicazione dell'avvenuto pagamento, annotando sui singoli mandati "a copertura del sospeso n._____" rilevabile dal giornale di cassa fornito dal Tesoriere.

I beneficiari dei pagamenti potranno essere avvisati direttamente dall'Azienda dopo l'avvenuta consegna dei relativi mandati al Tesoriere.
I pagamenti verranno eseguiti dal Tesoriere nell'ambito della disponibilità di cassa, ivi compresa l'anticipazione di cui al successivo punto G del presente articolo.
Il Tesoriere non può dar corso al pagamento dei mandati irregolari, incompleti o che presentino discordanze fra la somma scritta in lettere e quella in cifre. Qualora il pagamento debba essere effettuato a data fissa od abbia un termine determinato, ne dovrà essere fatta espressa indicazione sul mandato a cura dell'Azienda. E' vietato il pagamento di mandati provvisori od annuali complessivi.
I mandati sono pagabili, di norma, agli sportelli del Tesoriere contro ritiro di regolare quietanza, in tal caso non sono previste spese a carico dei beneficiari.
Ai pagamenti il Tesoriere potrà provvedere, se espressamente richiesto dal beneficiario dell'Azienda, con annotazione riportata sui mandati, anche mediante corrispondente somma contante entro i limiti di legge e nel rispetto della normativa vigente in materia di tracciabilità dei flussi finanziari, con vaglia postale, con c/c postale e con accredito in c/c bancario, comprovando i pagamenti effettuati con l'annotazione del Tesoriere o rispettivamente con la copia dell'ordine di bonifico, con la ricevuta rilasciata dall'Amministrazione delle Poste e con la copia della contabile di accredito, in tali casi tutte le spese e commissioni previste per l'esecuzione di tali pagamenti verranno addebitate al beneficiario
Qualora siano emessi mandati di pagamento riferiti ad uno stesso beneficiario ed aventi la stessa data essi dovranno essere raggruppati in un unico pagamento, anche ai fini dell'applicazione di commissioni.
I mandati saranno consegnati al Tesoriere di norma 5 giorni lavorativi, prima di quello fissato per il pagamento e riportato sul mandato stesso, qualora non sia indicata la data di scadenza del pagamento esso dovrà avvenire entro il 5° giorno lavorativo successivo alla trasmissione del mandato.
<u>In particolare i pagamenti relativi alle retribuzioni del personale dipendente</u>:

- dovranno essere accreditati il giorno 27 di ogni mese o essere anticipati all'ultimo giorno lavorativo antecedente qualora tale data cada in giornata festiva o non lavorativa; per il mese di dicembre la data di riferimento sarà comunicata dall'Azienda, e sarà comunque collocata fra il giorno 10 ed il giorno 18
- dovranno essere effettuati con accrediti diretti sul conto corrente bancario o postale dei beneficiari o presso uno o più sportelli del Tesoriere, preventivamente individuati di concerto con l'Azienda
- dovranno essere effettuati con valuta fissa
- non dovranno comportare onere finanziario a carico dell'Azienda o dei suoi dipendenti
- l'Azienda trasmetterà al Tesoriere l'elenco dei beneficiari entro il 5° giorno lavorativo antecedente a quello del pagamento degli stipendi e successivamente trasmetterà i relativi mandati
- Il Tesoriere ha l'obbligo di rispettare le condizioni sopraindicate anche in caso di sciopero del proprio personale, in quanto trattasi di prestazioni essenziali ai sensi della Legge 12.6.1990 n. 146 art.1 comma 2 lett. c e ss.mm. ed ii.

Su richiesta dell'Azienda, il Tesoriere si obbliga di curare la domiciliazione gratuita delle utenze (luce, gas, telefono, acqua, rifiuti) ad essa intestate.

Il Tesoriere provvederà a commutare d'ufficio in assegni postali localizzati, o con altri mezzi equipollenti offerti dal sistema bancario e postale i mandati di pagamento individuali o collettivi che dovessero rimanere interamente o parzialmente inestinti alla chiusura dell'esercizio, con spese a carico del beneficiario. Qualora le spese e le tasse inerenti all'esecuzione dei pagamenti sopra descritti siano poste dall'Azienda a carico dei beneficiari, il Tesoriere sarà autorizzato a trattenere dall'importo nominale del mandato l'ammontare delle spese in questione ed alla mancata corrispondenza fra la somma definitivamente versata e quella del mandato medesimo sopperirà formalmente l'indicazione sul titolo, sia dell'importo delle spese che del netto pagato. I mandati, accreditati o comunicati con

l'osservanza di quanto sopra stabilito nel presente articolo, si considerano titoli pagati agli effetti del conto consuntivo. L'Azienda si impegna a non presentare al Tesoriere mandati oltre la data, del mese di chiusura esercizio, concordata preventivamente con il Tesoriere , ad eccezione di quelli relativi ai pagamenti aventi scadenza perentoria successiva a tale data.

D) IMPOSTE VIGENTI

Tanto i mandati di pagamento, quanto gli ordini di riscossione, siano essi reversali od elenchi, debbono recare l'indicazione se le operazioni in esse ordinate, siano o meno, da assoggettarsi all'imposta di bollo.

E) TRASMISSIONE ORDINATIVI

Gli ordinativi d'incasso (reversali) e di pagamento (mandati) saranno trasmessi telematicamente dall'Azienda al Tesoriere in ordine cronologico e progressivo accompagnati da distinta, di cui il Tesoriere tiene specifico elenco

F) FIRME AUTORIZZATE

L'Azienda dovrà comunicare preventivamente al Tesoriere le generalità e qualifiche nonché trasmettere le firme autografe e digitali delle persone autorizzate ad operare sul Conto Corrente di Tesoreria, firmare gli ordini di riscossione e di pagamento nonché, tempestivamente, le eventuali variazioni che potranno intervenire per decadenza e nomina, corredando le comunicazioni stesse delle copie delle deliberazioni degli Organi competenti che hanno conferito i poteri di cui sopra. Il Tesoriere resterà impegnato dal giorno lavorativo successivo a quello di ricezione delle comunicazioni stesse. Nel caso in cui gli ordinativi di riscossione e spesa siano firmati dai sostituti, s'intende che l'intervento dei medesimi è dovuto all'assenza od all'impedimento dei titolari.

G) ANTICIPAZIONE DI TESORERIA - TASSO DEBITORE

Il Tesoriere è tenuto a dar corso ai pagamenti esclusivamente a valere e fino alla concorrenza delle disponibilità di cassa giacenti presso se stesso, esaurite le quali ne darà avviso all'Azienda. Il Tesoriere su richiesta dell'Azienda presentata di norma a inizio dell'esercizio e corredata dalla Deliberazione del Consiglio di Amministrazione s'impegna ad accordare all'Azienda anticipazioni di cassa sino ad un importo complessivo non superiore ai 3/12 delle entrate effettive accertate dell'ultimo bilancio approvato, o ad altro limite stabilito dalla normativa tempo per tempo vigente. L'anticipazione concorre a sopperire a momentanee esigenze di cassa e viene utilizzata limitatamente alle somme necessarie. L'Azienda è tenuta a corrispondere al Tesoriere sui saldi debitori giornalieri un tasso d'interesse pari all'Euribor 3 mesi (tasso 365) riferito alla media mese precedente aumentato/diminuito dello spread offerto in sede di gara, senza applicazione di commissione per massimo scoperto. I suddetti interessi, per i quali l'Azienda avrà istituito apposito conto in bilancio, verranno calcolati limitatamente all'effettivo utilizzo ed addebitati sul c/c di tesoreria con liquidazione annuale. Il Tesoriere avrà diritto a rivalersi delle anticipazioni concesse su tutte le entrate dell'Azienda fino a totale compensazione delle somme anticipate.
In caso di cessazione del servizio, per qualsiasi motivo, l'Azienda si impegna ad estinguere immediatamente ogni e qualsiasi esposizione debitoria derivante da eventuali anticipazioni e finanziamenti, anche con cadenza predeterminata, concessi dal Tesoriere a qualsiasi titolo, obbligandosi, in via subordinata a far rilevare dal Tesoriere subentrante, alla data di inizio del servizio le anzidette esposizioni, nonché a far assumere tutti gli obblighi inerenti ad eventuali impegni di firma rilasciati nell'interesse dell'Azienda dal Tesoriere uscente.

H) GIACENZE DI CASSA - TASSO CREDITORE

Sulle giacenze di cassa e sui depositi di somme in genere esistenti presso il Tesoriere, saranno da questi corrisposti all'Azienda gli interessi creditori commisurati ad un tasso d'interesse pari all'Euribor

3 mesi (tasso 365) riferito alla media mese precedente aumentato/diminuito dello spread offerto in sede di gara . Detti interessi saranno accreditati, al netto delle ritenute di legge, sul conto di tesoreria con liquidazione annuale.
Qualora il tasso di interesse creditore risulti negativo, non potranno, in ogni caso essere addebitati interessi negativi.
Agli effetti del conteggio degli interessi, sia attivi che passivi per l'Azienda, il Tesoriere dovrà tenere aggiornato il conto scalare di cui copia dovrà essere rimessa all'Azienda. A chiusura periodica il Tesoriere trasmetterà all'Azienda l'ultimo foglio dell'estratto conto regolato per capitali ed interessi.
L'Azienda si riserva di impiegare le somme eccedenti gli ordinari bisogni in investimenti fruttiferi anche presso altri Istituti.
Le somme riscosse o pagate saranno portate a credito o a debito sul c/c di tesoreria dell'Azienda con le valute sottoindicate:
Valute sulle riscossioni:

- contanti, assegni circolari , assegni su piazza e fuori piazza: stesso giorno dell'operazione.
- Bonifici bancari : giorno successivo all'incasso

Valute sui pagamenti:

- stesso giorno dell'operazione di pagamento
- per i pagamenti a valuta fissa al beneficiario: il giorno di valuta prefissata

I) AMMINISTRAZIONE TITOLI E VALORI IN DEPOSITO

Il Tesoriere assumerà in custodia ed amministrazione i titoli ed i valori di proprietà dell'Azienda a titolo gratuito. Alle condizioni suddette, saranno altresì custoditi ed amministrati i titoli ed i valori depositati da terzi per cauzione a favore dell'Azienda con l'obbligo, per il Tesoriere, di non procedere alla restituzione degli stessi senza regolari ordini dell''Azienda comunicati per iscritto e sottoscritti dalle persone autorizzate a firmare i titoli di spesa.

L) OBBLIGHI DELL'AZIENDA

L'Azienda si obbliga a trasmettere al Tesoriere per ogni esercizio il Bilancio Preventivo ed il Bilancio Consuntivo approvati.

M) OBBLIGHI DEL TESORIERE

Il Tesoriere deve tenere aggiornato e custodire:

- il giornale di cassa sul quale registrerà, in ordine cronologico, ogni riscossione ed ogni pagamento, copia di detto giornale, con l'indicazione delle risultanze di cassa, verrà inviato giornalmente all''Azienda;
- il bollettario delle riscossioni;
- gli ordinativi finanziari cronologicamente ordinati;
- eventuali altre evidenze previste dalla legge.

Il Tesoriere deve inoltre restituire all'Azienda documenti e quietanze inerenti pagamenti relativi ad obblighi contributivi e fiscali, nei tempi previsti per le conseguenti dichiarazioni o verifiche.

N) QUADRO DI RACCORDO DEL CONTO

L'Azienda consente che il tesoriere proceda, quando quest'ultimo lo ritenga opportuno, al raccordo delle risultanze della propria contabilità con quelle della contabilità dell'Azienda stessa. L'Azienda deve dare il relativo benestare al Tesoriere, oppure segnalare le discordanze eventualmente rilevate, entro e non oltre 30 giorni dalla data d'invio del quadro di raccordo; trascorso tale termine, il Tesoriere resta sollevato da ogni responsabilità derivante dalla mancata o ritardata segnalazione delle discordanze emerse dalla verifica.

O) VERBALE DI CASSA

Il Tesoriere, entro tre mesi dalla chiusura dell'esercizio, dovrà rassegnare il verbale di verifica di cassa redatto in conformità delle relative disposizioni di legge.

P) GARANZIA PER LA GESTIONE DEL SERVIZIO

Il Tesoriere risponderà di tutte le somme e di tutti i valori dallo stesso trattenuti in deposito ed in consegna per conto dell'Azienda, nonché per tutte le operazioni comunque attinenti al servizio.
Nessuna responsabilità o gravame potrà addossarsi al Tesoriere, in tutti i casi in cui, la chiusura dell'Ufficio di Tesoreria od il non regolare svolgimento del servizio affidatogli, sia dovuto a cause di forza maggiore.

Q) SEDE OPERATIVA

Il Tesoriere dovrà costituire all'attivazione del servizio sede operativa nel Comune di Reggio Emilia, in essa dovrà operare personale con esperienza lavorativa pregressa dimostrabile nei servizi di Tesoreria.

R) CONSEGNA VALORI

Il Tesoriere si impegna a consegnare presso la sede amministrativa dell'Azienda le somme corrispondenti ai mandati da quietanzarsi da parte dell'Economo, mediante consegne a cadenza indicativamente quindicinale di importo indicativamente contenuto entro la somma di Euro 15.000,00.

S) COLLEGAMENTO INFORMATICO – TELEMATICO, GESTIONE INFORMATIZZATA DEGLI INCASSI E ADEMPIMENTI CONNESSI

Quanto di seguito descritto è da intendersi come modalità di resa del servizio di tesoreria.
Il Tesoriere si impegna a garantire, rendendolo disponibile fin dall'assunzione del servizio, un sistema informatizzato del servizio (Remote banking) con possibilità di contemporaneo accesso ed utilizzo da parte di più utenti dell'Azienda, preventivamente identificati ed autorizzati, senza oneri né in fase di implementazione che per successivi aggiornamenti e/o manutenzioni; il sistema informatizzato, che potrà essere oggetto di separato protocollo tecnico-operativo fra l'Azienda ed il Tesoriere, dovrà consentire di ricevere informazioni su movimenti e saldi inerenti il conto corrente intestato all'Azienda, di inviare e ricevere flussi di dati inerenti incassi e pagamenti, di inviare gli ordinativi di incasso e pagamento informatici sottoscritti digitalmente, e dovrà permettere di effettuare direttamente quelle operazioni la cui esecuzione fosse richiesta per legge o ritenuta opportuna dall'Azienda, quali versamenti di imposte o trasmissione di modelli fiscali. La mancata attivazione oltre 30 giorni dall'avvio del servizio, potrà configurare causa di risoluzione contrattuale per inadempimento.

Il Tesoriere si impegna ad attivare contestualmente all'assunzione del servizio di tesoreria le procedure informatiche idonee a consentire la riscossione delle entrate rette, tariffe, contribuzioni varie, canoni di locazione sulla base dei dati trasmessi dall'Azienda in via telematica garantendo:

- incasso delle somme corrispondenti mediante sistema bancario con addebito in conto corrente del debitore dei SEPA relativi ai flussi inviati da ASP e relativo accredito delle somme sul conto corrente di tesoreria
- disponibilità della rendicontazione riferita a tali incassi
- restituzione dei dati riferiti a tali incassi mediante invio telematico in formato leggibile dal software in uso all'Azienda in modo da consentirne acquisizione automatica

Tali procedure dovranno essere attivate contestualmente all'assunzione del servizio di tesoreria; eventuali adeguamenti dei programmi informatici che si rendessero necessari al fine di garantire quanto precedentemente indicato, dovranno essere senza oneri per l'Azienda; le specifiche di tali procedure potranno essere oggetto di separato protocollo tecnico-operativo fra l'Azienda ed il

Tesoriere. Il rimborso dei costi di tale servizio sarà commisurato al valore offerto in sede di gara. La mancata attivazione oltre 30 giorni potrà configurare causa di risoluzione contrattuale per inadempimento.

Il Tesoriere si impegna ad attivare contestualmente all'assunzione del servizio di tesoreria le procedure informatiche idonee a consentire la gestione degli incassi tramite il sistema nazionale degli incassi della Pubblica Amministrazione, PagoPA, cui l'Azienda ha aderito nominando un partner tecnologico ed interfacciando i gestionali in uso.
Tali procedure dovranno essere attivate contestualmente all'assunzione del servizio di tesoreria; eventuali adeguamenti dei programmi informatici che si rendessero necessari al fine di garantire quanto precedentemente indicato, dovranno essere senza oneri per l'Azienda; il Tesoriere dovrà disporre, in proprio o attraverso un proprio fornitore, di un'adeguata piattaforma software, per mezzo della quale dovrà essere in grado di consentire all'Azienda – operando in qualità di "Partner Tecnologico" di gestire le proprie entrate in conformità con gli standard normativi, integrando altresì, a propria cura e spese, tale piattaforma con il software applicativo in uso in Azienda .
Relativamente agli incassi tramite il sistema PagoPa il Tesoriere dovrà permettere la riconciliazione automatica delle posizioni creditorie con i pagamenti effettuati e con i relativi incassi sul conto corrente di Tesoreria rendicontati nel giornale di cassa.
Le specifiche di tali procedure potranno essere oggetto di separato protocollo tecnico-operativo fra l'Azienda ed il Tesoriere. Il rimborso dei costi di tale servizio sarà commisurato al valore offerto in sede di gara. La mancata attivazione oltre 30 giorni potrà configurare causa di risoluzione contrattuale per inadempimento

Il Tesoriere si impegna ad adeguare le proprie procedure informatiche e/o a predisporre software di collegamento senza oneri per l'Azienda, al fine di trasmettere i dati relativi a riscossioni e pagamenti avvenuti ed accogliere i dati elaborati dalle procedure informatiche dell'Azienda, ciò, in particolare al fine di consentire all'Azienda di inviare ed autorizzare gli ordinativi di pagamento e di incasso in via esclusivamente telematica certificati da firma digitale, conformemente alle disposizioni legislative in materia: in particolare la gestione dell'ordinativo elettronico con apposizione di firma digitale dovrà essere attivato contestualmente all'assunzione del servizio di tesoreria, potrà essere disciplinato in apposito protocollo-tecnico operativo concordato e sottoscritto dall'Azienda e dal Tesoriere. La mancata attivazione oltre 30 giorni dall'assunzione del servizio di tesoreria potrà configurare causa di risoluzione contrattuale per inadempimento.

Il Tesoriere provvederà gratuitamente in nome e per conto dell'Azienda all'archiviazione e alla conservazione sostitutiva dei documenti informatici relativi al servizio di tesoreria sottoscritti con firma digitale, per il periodo minimo prescritto dalla legge , ai sensi del d.lgs. n. 82/2005, ovvero, a richiesta dell'Azienda provvederà alla trasmissione gratuita e periodica di tutti i documenti informatici prodotti nel corso del servizio di tesoreria al ParER, Polo archivistico regionale, nell'ambito di quanto previsto dalle L.R. 11/2004 e L.R. 17/2013.

ART.3
VARIANTI IN ESECUZIONE DI CONTRATTO- REVISIONE PREZZI

Sono ammesse "Varianti in corso di esecuzione contrattuale" così come regolamentate dai commi 12 (aumento o diminuzione fino a concorrenza del quinto) e 11 (modifica della durata – proroga) dell'art. 106 D.lgs 50/2016, oltre le restanti varianti contemplate dal medesimo articolo , comma 1 lett a) revisione prezzi sulla base di quanto previsto negli atti di gara , lett e) modifiche non sostanziali, nonché in relazione anche situazioni impreviste e imprevedibili, per nuove disposizioni legislative (c.d. varianti in corso d'opera).

ART. 4
VERIFICHE / ISPEZIONI

L'Azienda avrà diritto di procedere a verifiche di cassa e dei valori dati in custodia ogni qualvolta lo riterrà necessario ed opportuno.
Il Tesoriere dovrà all'uopo esibire, ad ogni richiesta, i registri, i bollettari e tutta la documentazione contabile relativa alla gestione del Servizio in oggetto.
Il Tesoriere è tenuto a prestarsi alle verifiche che potranno essere richieste dagli Organi di Controllo dell'Azienda, in base alla normativa vigente in materia.

ART. 5
DURATA –PERIODO DI PROVA - PROROGA – CESSAZIONE DAL SERVIZIO- SUBAPPALTO

"Durata"

L'appalto avrà durata di 36 mesi, eventualmente rinnovabili.

"Periodo di prova"

Per i primi sei mesi l'affidamento del servizio si intenderà conferito a "titolo di prova" al fine di consentire al committente una valutazione ampia e complessiva sul servizio reso.
Durante tale periodo il committente potrà recedere, in caso di valutazione negativa, ai sensi di quanto disposto dall'art. 1373 del Codice Civile, mediante semplice "Comunicazione scritta" adeguatamente motivata e con preavviso di 15 giorni. In tal caso all'impresa non spetterà alcun indennizzo.

"Proroga"

Se allo scadere del termine naturale del contratto, l'Aziende non dovesse aver aggiudicato il servizio per il periodo successivo, l'assegnataria risulterà tenuta a continuarlo in regime di proroga, pertanto alle medesime condizioni, per la durata di mesi 6, o comunque in misura "strettamente necessaria nelle more di svolgimento delle ordinarie procedure di scelta del contraente". Trattasi di proroga tecnica ex comma 11 art. 106 D.Lgs 50/16, opzione contemplata all'intento dei documenti di gara.

"Cessazione dal Servizio"

All'atto della cessazione del servizio, il Tesoriere è tenuto a consegnare all'Azienda, allegati alla documentazione di sua competenza, tutti i registri, i bollettari e quant'altro si riferisca alla gestione del servizio, in qualunque momento ciò abbia a verificarsi.

In caso di cessazione dal servizio le somme che fossero erroneamente versate a favore dell'Azienda ricevute dal Tesoriere cessante, saranno da questi trasferite senza oneri al Tesoriere subentrante.

"Sub appalto"

Il subappalto è ammesso nei limiti di legge e di quanto indicato in sede di offerta, previa autorizzazione dell'Azienda. In caso di mancata indicazione il subappalto è vietato.

ART. 6
CORRISPETTIVO - RIMBORSI SPESE – TRACCIABILITA'

Il Servizio di Tesoreria, così come contemplato agli artt. 2 e 3 del presente Capitolato, si intenderà erogato a titolo gratuito.

L'Azienda si impegna ad onorare i rimborsi inerenti:

- spese e diritti postali;
- bolli di quietanza dovuti dall'Azienda;
- oneri fiscali sostenuti dal Tesoriere in dipendenza della gestione degli stessi;
- spese inerenti il servizio di riscossione entrate come descritto all'art. 2 lett S in misura corrispondente a quanto offerto in sede di gara.
- spese per operazioni e servizi accessori derivanti dal Servizio in oggetto e/o in esso non espressamente previsti in misura da concordarsi caso per caso fra l'Azienda ed il Tesoriere

In relazione al Servizio di Tesoreria gli obblighi di tracciabilità di cui alla L. 136/2010 e s.m.e. si considerano assolti con l'acquisizione del CIG al momento della procedura di affidamento.

ART. 7
ONERI DERIVANTI DAL RAPPORTO DI LAVORO - RISCHI DA INTERFERENZA

Il Tesoriere dovrà osservare verso i propri dipendenti, ogni legge, regolamento e disposizione normativa in materia di rapporto di lavoro, previdenza / assistenza, assicurazione contro gli infortuni, nonché di sicurezza ed igiene nei luoghi di lavoro (D.lgs 81/2008 sue integrazioni e modificazioni). Non si rilevano rischi da interferenza, né conseguentemente costi della sicurezza.

Il Tesoriere dovrà inoltre applicare verso i propri dipendenti un trattamento economico e normativo non inferiore a quello risultante dal contratto collettivo nazionale di categoria applicabile e dagli accordi integrativi territoriali vigenti nella località di esecuzione del Servizio, sottoscritti dalle Organizzazioni Sindacali più rappresentative.

Il Tesoriere dovrà infine applicare ogni disposizione normativa, nessuna esclusa, inerente gli eventuali obblighi verso i lavoratori dell'Impresa cessante.

L'assolvimento degli obblighi di cui sopra rappresenta condizione indispensabile ed irrinunciabile per la sottoscrizione e la successiva validità del contratto.

Trattandosi di servizi di natura intellettuale in sede di gara non verranno richiesti i costi di sicurezza aziendali né i costi della manodopera.

Art. 8
CODICE DI COMPORTAMENTO

Il Tesoriere si impegna ad osservare, a rendere edotti e a fare osservare ai propri dipendenti, *consulenti e collaboratori, nonché subappaltatori e dipendenti, consulenti e collaboratori di questi ultimi* per quanto compatibile con il ruolo e l'attività svolta in ordine al contratto di cui alla presente procedura, gli obblighi di condotta previsti dal Codice di comportamento dei dipendenti pubblici di cui al D.P.R. N. 62/2013 nonché quelli previsti dal Codice di comportamento dei dipendenti dell'ASP REGGIO EMILIA Città delle Persone, approvato con deliberazione del C.d.A. n. 2016/16 del 12.04.2016 .

A tal fine dell'ASP REGGIO EMILIA Città delle Persone comunica che tali documenti sono pubblicati sul sito internet aziendale : www.asp.re.it/Amministrazione trasparente/Disposizioni generali/Atti generali/Codici disciplinari .

ART. 9

CONTINUITA' DEL SERVIZIO

Il Tesoriere, in caso di sciopero, è tenuto a garantire le prestazioni essenziali individuate all'art. 1, comma 2 lett c) della legge 12.06.1990 n. 146 e ss.mm. ed ii. ai fini della continuità dell'erogazione di emolumenti retributivi o comunque di quanto economicamente necessario al soddisfacimento delle necessità della vita attinenti a diritti alla persona costituzionalmente garantiti.

In relazione a quanto sopra, il tesoriere è tenuto a trasmettere entro 30 giorni dalla stipula del contratto di cui alla presente procedura gli accordi sindacali o i regolamenti previsti dall'art. 2 della citata legge 146/1990 indicanti le prestazioni minime garantite, le modalità e le procedure di erogazione e le altre misure dirette a consentire gli adempimenti di cui sopra.

ART. 10

INADEMPIENZE – PENALI - RISOLUZIONE CONTRATTUALE –RECESSO

Il Tesoriere dovrà realizzare il servizio nel pieno rispetto della normativa prevista in materia e di quanto disposto dal presente contratto .

L'Azienda si riserva la facoltà di avanzare risoluzione contrattuale ai sensi di quanto disposto dall'art. 1456 c.c "Clausola Risolutiva Espressa" , tramite semplice dichiarazione stragiudiziale intimata a mezzo lettera raccomandata A/R nel caso in cui si verifichino gravi inadempienze, quali:

- inosservanza delle disposizioni normative;
- gravi inadempienze che abbiano arrecato importante disagio o disservizio al committente od ai propri dipendenti/creditori ;
- reiterate contravvenzioni agli obblighi ed alle condizioni contrattuali;
- subappalto del servizio se non indicato in sede di offerta e non autorizzato;
- interruzione del servizio senza giustificato motivo
- inottemperanza alle norme per la sicurezza nell'ambiente di lavoro
- fallimento, avvio della procedura per il concordato preventivo o altra procedura concorsuale che dovesse travolgere il Tesoriere;

Nei casi di :

- mancato rispetto delle condizioni di valuta
- mancato rispetto dei termini di pagamento dei mandati
- mancato funzionamento degli sportelli in circolarità

l'Azienda applicherà la penale di Euro 100,00 per ogni singola violazione.

In caso di eventuali altre inadempienze diverse da quelle sopra elencate l'Azienda applicherà penali da Euro 100,00 a Euro 1.000,00, a proprio insindacabile giudizio graduando la penale a seconda della gravità dell'inadempimento

In caso venissero riscontrati inadempimenti contrattuali l'Azienda procederà alla trasmissione di specifica contestazione al Tesoriere a mezzo PEC. La comunicazione conterrà l'esatta descrizione delle circostanze contestate e della penale applicata, ovvero potrà contenere intimazione ad adempiere, o, infine assegnare un termine non inferiore a quindici giorni, per la presentazione da parte del Tesoriere di controdeduzioni e osservazioni.

L'Azienda avrà facoltà, previa intimazione scritta ad adempiere, di risolvere il contratto con tutte le conseguenze di Legge e di Contratto che la risoluzione comporta, ivi compresa la facoltà di affidare il servizio a terzi in danno della ditta, fatto salvo il diritto d'azione per il risarcimento dell'eventuale maggior danno subito.

L'applicazione delle penali non pregiudica eventuali azioni di risarcimento per maggior danno subito, derivante dall'inadempimento contrattuale.

L'Azienda avrà piena discrezionalità di procedere a risoluzione contrattuale indipendentemente dall'aver o meno, comminato penali.
In seguito alla risoluzione per inadempimento del Tesoriere, l'Azienda si riserva il diritto, ove possibile, di procedere con scorrimento della graduatoria ed in subordine attraverso le modalità consentite dall'ordinamento giuridico.

In caso di riaffidamento del servizio a seguito di risoluzione per inadempienza del Tesoriere, si darà applicazione a quanto disposto dall'art. 110 del D.Lgs 50/2016 e l'affidamento per scorrimento di graduatoria avverrà alle condizioni "già proposte dall'originario aggiudicatario in sede di offerta"

L'Azienda si riserva inoltre la facoltà di recedere ex art. 1 comma 13 del D.L. 2012/95 (spending review) come convertito dalla L. 2012/135, qualora a contratto stipulato, i parametri delle convenzioni delle Centrali di Committenza sopraggiunte, risultino migliorative rispetto al contratto in corso e qualora l'aggiudicataria non acconsenta ad una modifica delle condizioni economiche tali da rispettare il limite di cui all'art. 26 comma 3 della L. 1999/488.

ART. 11
STIPULA CONTRATTO - SPESE

Il contratto verrà stipulato in modalità elettronica mediante scrittura privata sottoscritta digitalmente.

Il contratto sarà oggetto a registrazione solo in caso d'uso ai sensi di quanto disposto dall'art. 5 comma 2 del DPR 26.04.86 n. 131, con onere a carico della parte richiedente la registrazione.

Il contratto, è assoggettato, con onere a carico del Tesoriere ad imposta di bollo ai sensi dell'art. 2, della tariffa, parte prima, allegata al D.P.R. 26 ottobre 1972, n. 642" in modo virtuale o mediante versamento all'intermediario convenzionato con l'Agenzia delle Entrate che ne rilascia apposito contrassegno. L'assolvimento andrà ottemperato e dimostrato.

ART. 12
RINVIO

Per quanto non qui esplicitamente previsto, al presente contratto si applica la normativa in tema di contratti delle pubbliche amministrazioni, in tema di contabilità degli enti pubblici non economici e delle Aziende Pubbliche di Servizi alla Persona, in tema di materie bancarie e creditizie, in tema di digitalizzazione della pubblica amministrazione, nonché la normativa vigente.

ART. 13
FORO COMPETENTE

Per eventuali controversie che dovessero insorgere durante la vigenza contrattuale sarà competente il Foro di Reggio Emilia.

ART. 14
TUTELA DELLA RISERVATEZZA DEI DATI PERSONALI

Il Tesoriere ha l'obbligo di mantenere riservati i dati e le informazioni, ivi comprese quelle che transitano per le apparecchiature di elaborazione dati, di cui venga in possesso e comunque a conoscenza, anche tramite

l'esecuzione del contratto, di non divulgarli in alcun modo e in qualsiasi forma, di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione del Contratto e di non farne oggetto di comunicazione o trasmissione senza l'espressa autorizzazione dell'Azienda.
L'obbligo di cui al precedente comma sussiste, altresì, relativamente a tutto il materiale originario o predisposto in esecuzione del Contratto.
Gli obblighi di cui sopra non concernono i dati che siano o divengano di pubblico dominio.
Il Tesoriere è responsabile per l'esatta osservanza da parte dei propri dipendenti, consulenti e collaboratori, nonché di subappaltatori e dei dipendenti, consulenti e collaboratori di questi ultimi, degli obblighi di segretezza di cui ai commi precedenti e risponde nei confronti dell'Azienda per eventuali violazioni dell'obbligo di riservatezza commesse dai suddetti soggetti.
Il Tesoriere può utilizzare servizi di cloud pubblici ove memorizzare i dati e le informazioni trattate nell'espletamento dell'incarico affidato, solo previa autorizzazione dell'Azienda.
In caso di inosservanza degli obblighi descritti nei punti precedenti, l'Azienda ha facoltà di dichiarare risolto di diritto il Contratto, fermo restando che il Tesoriere sarà tenuto a risarcire tutti i danni che ne dovessero derivare. Il Tesoriere potrà citare i termini essenziali del Contratto nei casi in cui fosse condizione necessaria per la partecipazione del il Tesoriere stesso a gare e appalti, previa comunicazione all'Azienda delle modalità e dei contenuti di detta citazione.
Sarà possibile ogni operazione di auditing da parte dell'Azienda attinente le procedure adottate dal Tesoriere in materia di riservatezza e degli altri obblighi assunti con il contratto.
I dati personali oggetto del servizio saranno utilizzati esclusivamente per lo svolgimento delle attività previste dal contratto, nel rispetto di quanto previsto dal Regolamento (UE) 2016/679 sulla protezione dei dati personali e dal D. Lgs. 196/2003. Il Tesoriere si impegna in ogni caso ad adottare e mantenere appropriate misure di sicurezza, sia tecniche che organizzative, per proteggere i dati personali da eventuali distruzioni o perdite di natura illecita o accidentale, danni, alterazioni, divulgazioni o accessi non autorizzati, ed in particolare, laddove il trattamento comporti trasmissioni di dati su una rete, da qualsiasi altra forma illecita di trattamento.
Il Tesoriere si impegna inoltre ad adottare misure tecniche ed organizzative adeguate per salvaguardare la sicurezza di qualsiasi rete di comunicazione elettronica o dei servizi forniti al committente, con specifico riferimento alle misure intese a prevenire l'intercettazione di comunicazioni o l'accesso non autorizzato a qualsiasi computer o sistema.
ASP è Titolare del trattamento di tali dati e provvede a nominare il Tesoriere "Responsabile del trattamento" mediante la stipula dell'allegato accordo recante le finalità, i contenuti e le condizioni indicate dall'art. 28, commi 3 e ss. del suddetto Regolamento Europeo. (Allegato 1)
In particolare, sottoscrivendo tale accordo il Tesoriere garantisce l'adozione di misure tecniche e organizzative adeguate affinché il trattamento dei dati personali che gli sono affidati dal Titolare ASP sia conforme ai requisiti del Regolamento e sia idoneo a tutelare i diritti degli interessati, secondo le indicazioni che verranno comunicate dal Committente.
In caso di inadempimento, il Tesoriere sarà considerato responsabile nei confronti del Titolare ai sensi di legge.
In caso il Tesoriere si avvalga di incaricati o collaboratori, dovrà renderli edotti delle suddette norme operative generali, fermo restando che in ogni caso essi devono operare sotto la sua diretta ed esclusiva responsabilità.
Quale designato Responsabile del trattamento dati personali, il Tesoriere, in coerenza con quanto previsto dalla normativa richiamata (art. 28 GDPR 2016/679) dovrà:

- adempiere all'incarico attribuito adottando idonee e preventive misure di sicurezza, con particolare riferimento a quanto stabilito dall'art. 32 Regolamento UE/2016/679 (GDPR);
- predisporre, qualora l'incarico comprenda la raccolta di dati personali, l'informativa di cui all'art 13 del Regolamento UE/2016/679 (GDPR) e verificare che siano adottate le modalità operative necessarie affinché la stessa sia effettivamente portata a conoscenza degli interessati;
- dare direttamente riscontro orale, anche tramite propri incaricati, alle richieste verbali dell'interessato;
- trasmettere ad ASP, con la massima tempestività, le istanze dell'interessato per l'esercizio dei diritti di cui agli artt. 7 e da 15 a 22 del Regolamento UE/2016/679 (GDPR) che necessitino di riscontro scritto, in modo da consentire all'ASP stessa di dare riscontro all'interessato nei termini; nel fornire altresì all'Azienda tutta l'assistenza necessaria, nell'ambito dell'incarico affidato, per soddisfare le predette richieste;
- individuare gli incaricati/autorizzati al trattamento dei dati personali, impartendo agli stessi le istruzioni necessarie per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite;

 consentire all'Azienda, in quanto Titolare del trattamento, l'effettuazione di verifiche periodiche circa il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, fornendo alla stessa piena collaborazione;

 osservare la policy Aziendale sul "data breach", allegato alla designazione a Responsabile del trattamento dati personali. . (Allegato 2)

IL DIRIGENTE AREA RISORSE
D.ssa Alessandra Sazzi

_____

TIMBRO DELL'IMPRESA E FIRMA
DEL LEGALE RAPPRESENTANTE

_____

Allegato 1 Accordo Responsabile del trattamento
Allegato 2 Policy aziendale sul "data breach"

Allegato 1)

Accordo Responsabile trattamento di dati personali

Il presente accordo costituisce allegato parte integrante del contratto siglato tra l'ASP REGGIO EMILIA Città delle Persone di seguito anche ASP o Azienda e il Fornitore di servizi, designato Responsabile del trattamento di dati personali ai sensi dell'art. 28 del GDPR.

1. Premesse

Il presente Accordo si compone delle clausole di seguito rappresentate e dai seguenti Allegati, che ne formano parte integrante e sostanziale:

● Allegato 1: Glossario

● Allegato 2: Appendice "Security"

Le Parti convengono quanto segue:

2. Trattamento dei dati nel rispetto delle istruzioni dell' ASP REGGIO EMILIA Città delle Persone

2.1 Il Fornitore, relativamente a tutti i Dati personali che tratta per conto dell' ASP REGGIO EMILIA Città delle Persone garantisce che:

● tratta tali Dati personali solo ai fini dell'esecuzione dell'oggetto del contratto, e, successivamente, solo nel rispetto di quanto eventualmente concordato dalle Parti per iscritto, agendo pertanto, esclusivamente sulla base delle istruzioni documentate e fornite dall'ASP;

● non trasferisce i Dati personali a soggetti terzi, se non nel rispetto delle condizioni di liceità assolte dall'ASP e a fronte di quanto disciplinato nel presente accordo;

● non tratta o utilizza i Dati personali per finalità diverse da quelle per cui è conferito l'incarico dall' ASP, financo per trattamenti aventi finalità compatibili con quelle originarie;

● prima di iniziare ogni trattamento e, ove occorra, in qualsiasi altro momento, informerà l' ASP se, a suo parere, una qualsiasi istruzione fornita dall'Azienda si ponga in violazione di Normativa applicabile;

2.2. Al fine di dare seguito alle eventuali richieste da parte di soggetti interessati, il Fornitore si obbliga ad adottare:

● procedure idonee a garantire il rispetto dei diritti e delle richieste formulate all'ASP dagli interessati relativamente ai loro dati personali;

● procedure atte a garantire l'aggiornamento, la modifica e la correzione, su richiesta dell' ASP dei dati personali di ogni interessato;

● procedure atte a garantire la cancellazione o il blocco dell'accesso ai dati personali a richiesta dall' ASP;

● procedure atte a garantire il diritto degli interessati alla limitazione di trattamento, su richiesta dell' ASP.

2.3 Il Responsabile del trattamento deve garantire e fornire all'Azienda cooperazione, assistenza e le informazioni che potrebbero essere ragionevolmente richieste dalla stessa, per consentirle di adempiere ai propri obblighi ai sensi della normativa applicabile, ivi compresi i provvedimenti e le specifiche decisioni del Garante per la protezione dei dati personali.

2.4 Il Responsabile del trattamento, anche nel rispetto di quanto previsto all'art. 30 del Regolamento, deve mantenere, compilare e rendere disponibile a richiesta della stessa, un registro dei trattamenti dati personali che riporti tutte le informazioni richieste dalla norma.

2.5 Il Responsabile del trattamento assicura la massima collaborazione al fine dell'esperimento delle valutazioni di impatto ex art. 35 del GDPR che l' ASP intenderà esperire sui trattamenti che rivelano, a Suo insindacabile giudizio, un rischio elevato per i diritti e le libertà delle persone fisiche.

3. Le misure di sicurezza

3.1 Il Responsabile del trattamento deve conservare i dati personali garantendo la separazione di tipo logico dai dati personali trattati per conto di terze parti o per proprio conto.

3.2 Il Responsabile del trattamento deve adottare e mantenere appropriate misure di sicurezza, sia tecniche che organizzative, per proteggere i dati personali da eventuali distruzioni o perdite di natura

illecita o accidentale, danni, alterazioni, divulgazioni o accessi non autorizzati, ed in particolare, laddove il trattamento comporti trasmissioni di dati su una rete, da qualsiasi altra forma illecita di trattamento.
3.3 Il Responsabile del trattamento fornisce al Titolare, nel caso di servizi di amministrazione di sistema forniti in insourcing, l'elenco con gli estremi identificativi delle persone fisiche che espleteranno, nell'ambito dell'incarico affidato funzioni di amministratori di sistema unitamente all'attestazione delle conoscenze, dell'esperienza, della capacità e dell'affidabilità degli stessi soggetti, i quali devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Si sottolinea che tale valutazione è propedeutica alla formale designazione ad amministratore di sistema da parte del Titolare il quale, in attuazione di quanto prescritto alla lettera f) del paragrafo 2 del Provvedimento del 28/11/2008 del Garante per la protezione dei dati personali relativo agli amministratori di sistema, provvederà alla registrazione degli accessi logici ai sistemi da parte degli amministratori di sistema designati;
3.4 Il Responsabile del trattamento deve adottare misure tecniche ed organizzative adeguate per salvaguardare la sicurezza di qualsiasi rete di comunicazione elettronica o dei servizi forniti all' ASP, con specifico riferimento alle misure intese a prevenire l'intercettazione di comunicazioni o l'accesso non autorizzato a qualsiasi computer o sistema.
3.5 Il Responsabile del trattamento adotta le misure di sicurezza di cui all'Appendice "Security" allegata al presente accordo. In ragione della riservatezza delle evidenze di analisi di conformità alle misure di cui alla suddetta Appendice, il Fornitore condivide con l' ASP tali informazioni solo in caso di violazione o data breach. Si sottolinea che, ad ogni buon conto, la sottoscrizione del presente accordo, e dei suoi allegati, equivale ad attestazione della conformità del Responsabile, e della soluzione informatica prodotta/sviluppata, alle misure indicate nell' appendice "Security".
3.6 Il Responsabile del trattamento dà esecuzione al contratto in aderenza alle politiche dell' ASP in materia di privacy e sicurezza informatica come indicate nelle policy aziendali ed eventuali successivi aggiornamenti delle medesime policy.
Le stesse sono consegnate a seguito della firma del presente accordo.

4. Analisi dei rischi, privacy by design e privacy by default

4.1 Con riferimento agli esiti dell'analisi dei rischi effettuata dall' ASP sui trattamenti di dati personali cui concorre il Fornitore, lo stesso assicura massima cooperazione e assistenza al fine di dare effettività alle azioni di mitigazione previste dall' ASP per affrontare eventuali rischi identificati.
4.2 Il Fornitore dovrà consentire all' ASP, tenuto conto dello stato della tecnica, dei costi, della natura, dell'ambito e della finalità del relativo trattamento, di adottare, sia nella fase iniziale di determinazione dei mezzi di trattamento, che durante il trattamento stesso, ogni misura tecnica ed organizzativa che si riterrà opportuna per garantire ed attuare i principi previsti in materia di protezione dati e a tutelare i diritti degli interessati.
4.3 In linea con i principi di privacy by default, dovranno essere trattati, per impostazione predefinita, esclusivamente quei dati personali necessari per ogni specifica finalità del trattamento, e che in particolare non siano accessibili dati personali ad un numero indefinito di soggetti senza l'intervento di una persona fisica.
4.4 Il Responsabile del trattamento dà esecuzione al contratto in aderenza alle policy di privacy by design e by default adottate dall' ASP e specificatamente comunicate.

5. Soggetti autorizzati ad effettuare i trattamenti - Designazione

5.1 Il Responsabile del trattamento garantisce competenze ed affidabilità dei propri dipendenti e collaboratori autorizzati al trattamento dei dati personali (di seguito anche incaricati) effettuati per conto dell' ASP.
5.2 Il Responsabile del trattamento garantisce che gli incaricati abbiano ricevuto adeguata formazione in materia di protezione dei dati personali e sicurezza informatica, consegnando all' ASP le evidenze di tale formazione.
5.3 Il Responsabile del trattamento, con riferimento alla protezione e gestione dei dati personali, impone ai propri incaricati obblighi di riservatezza non meno onerosi di quelli previsti nel Contratto

di cui il presente documento costituisce parte integrante. In ogni caso il Fornitore sarà direttamente ritenuto responsabile per qualsiasi divulgazione di dati personali dovesse realizzarsi ad opera di tali soggetti.

6. Sub-Responsabili del trattamento di dati personali

6.1 Il Fornitore, nell'eventualità di subappalto occorso ai sensi della normativa in materia di appalti e, per tutte le evenienze, nei casi di conferimento di parte del trattamento dei dati personali a soggetti terzi sub-responsabili, impone agli stessi condizioni vincolanti in materia di trattamento dei dati personali non meno onerose di quelle contenute nel presente Accordo.

6.2 Su specifica richiesta dell' ASP, il Fornitore dovrà provvedere a che ogni Sub-Responsabile sottoscriva direttamente con l' ASP un accordo di trattamento dei dati che, a meno di ulteriori e specifiche esigenze, preveda sostanzialmente gli stessi termini del presente Accordo.

6.3 In tutti i casi, il Fornitore si assume la responsabilità nei confronti dell' ASP per qualsiasi violazione od omissione realizzati da un Sub-Responsabile o da altri terzi soggetti incaricati dallo stesso, indipendentemente dal fatto che il Fornitore abbia o meno rispettato i propri obblighi contrattuali, ivi comprese le conseguenze patrimoniali derivanti da tali violazioni od omissioni.

7. Trattamento dei dati personali fuori dall'area economica europea

7.1 L' ASP non autorizza il trasferimento dei dati personali oggetto di trattamento al di fuori dell'Unione Europea.

8. Cancellazione dei dati personali

8.1 Il Fornitore provvede alla cancellazione dei dati personali trattati per l'esecuzione del presente contratto al termine del periodo di conservazione e in qualsiasi circostanza in cui sia richiesto dall' ASP, compresa l'ipotesi in cui la stessa debba avvenire per dare seguito a specifica richiesta da parte di interessati.

8.2 Alla cessazione del Contratto e, conseguentemente del presente Accordo, per qualsiasi causa avvenga, i dati personali dovranno, a discrezione dell' ASP, essere distrutti o restituiti alla stessa, unitamente a qualsiasi supporto fisico o documento contenente dati personali di proprietà dell' ASP.

9. Audit

9.1 Il Fornitore si rende disponibile a specifici audit in tema di privacy e sicurezza informatica da parte dell' ASP.

9.2 Il Fornitore consente, pertanto, all' ASP l'accesso ai propri locali e ai locali di qualsiasi Sub-Responsabile, ai computer e altri sistemi informativi, ad atti, documenti e a quanto ragionevolmente richiesto per verificare che il Fornitore, e/o i suoi Sub-fornitori, rispettino gli obblighi derivanti dalla normativa in materia di protezione dei dati personali e, quindi, da questo Accordo.

9.3 L'esperimento di tali audit non deve avere ad oggetto dati di terze parti, informazioni sottoposte ad obblighi di riservatezza degli interessi commerciali.

9.4 Nel caso in cui l'audit fornisca evidenze di violazioni alla normativa in materia di protezione dei dati personali e al presente Accordo, quali ad esempio quelle indicate all'art. 83 comma 5 del GDPR (con esclusione della lett. e) l'ASP può risolvere il Contratto o chiedere una cospicua riduzione del prezzo.

9.5 Nel caso in cui l'audit fornisca evidenze di violazioni gravi, quali ad esempio quelle indicate all'art. 83 comma 4 lett. a) del GDPR, l' ASP può chiedere una cospicua riduzione del prezzo.

9.6 Il rifiuto del Fornitore di consentire l'audit all' ASP comporta la risoluzione del contratto.

10. Indagini dell'Autorità e reclami

Nei limiti della normativa applicabile, il Fornitore o qualsiasi Sub-Responsabile informa senza alcun indugio l' ASP di qualsiasi:

- richiesta o comunicazione promanante dal Garante per la protezione dei dati personali o da forze dell'ordine;
- istanza ricevuta da soggetti interessati.

Il Fornitore fornisce, in esecuzione del contratto e, quindi, gratuitamente, tutta la dovuta assistenza all' ASP per garantire che la stessa possa rispondere a tali istanze o comunicazioni nei termini temporali previsti dalla normativa e dai regolamentari applicabili.

11. Violazione dei dati personali e obblighi di notifica

11.1 Il Fornitore, in virtù di quanto previsto dall'art. 33 del Regolamento, dovrà comunicare a mezzo di posta elettronica certificata all' ASP nel minor tempo possibile, e comunque non oltre 24 (ventiquattro) ore da quando ne abbia avuto notizia, qualsiasi violazione di sicurezza che abbia comportato 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, ivi incluse quelle che abbiano riguardato i propri sub-Fornitori. Tale comunicazione deve contenere ogni informazione utile alla gestione del *data breach*, oltre a:

● descrivere la natura della violazione dei dati personali;

● le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

● i recapiti del DPO nominato o del soggetto competente alla gestione del data breach;

● la descrizione delle probabili conseguenze della violazione dei dati personali;

● una descrizione delle misure adottate o che si intende adottare per affrontare la Violazione della sicurezza, compreso, ove opportuno, misure per mitigare i suoi possibili effetti negativi.

11.2 Il Fornitore deve fornire tutto il supporto necessario all' ASP ai fini delle indagini e sulle valutazioni in ordine alla violazione di dati, anche al fine di individuare, prevenire e limitare gli effetti negativi della stessa, conformemente ai suoi obblighi ai sensi del presente articolo e, previo accordo con l' ASP, per svolgere qualsiasi azione che si renda necessaria per porre rimedio alla violazione stessa. Il Fornitore non deve rilasciare, né pubblicare alcun comunicato stampa o relazione riguardante eventuali data breach o violazioni di trattamento senza aver ottenuto il previo consenso scritto dell' ASP.

12. Responsabilità e manleve

12.1 Il Fornitore tiene indenne e manleva l' ASP da ogni perdita, costo, sanzione, danno e da ogni responsabilità di qualsiasi natura derivante o in connessione con una qualsiasi violazione da parte del Fornitore delle disposizioni contenute nel presente Accordo.

12.2 A fronte della ricezione di un reclamo relativo alle attività oggetto del presente Accordo, il Fornitore:

● avverte, prontamente ed in forma scritta, l' ASP del Reclamo;

● non fornisce dettagli al reclamante senza la preventiva interazione con l' ASP;

● non transige la controversia senza il previo consenso scritto dell'ASP;

● fornisce all' ASP tutta l'assistenza che potrebbe ragionevolmente richiedere nella gestione del reclamo.

Allegato 1

GLOSSARIO

" **Garante per la protezione dei dati personali":** è l'autorità di controllo responsabile per la protezione dei dati personali in Italia;

" **Dati personali ":** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); 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;

" **GDPR" o "Regolamento":** si intende il Regolamento UE 2016/679 sulla protezione delle persone fisiche relativamente al trattamento dei dati personali e della loro libera circolazione (General Data Protection Regulation) che sarà direttamente applicabile dal 25 maggio 2018;

" **Normativa Applicabile":** si intende l'insieme delle norme rilevanti in materia protezione dei dati personali , incluso il Regolamento Privacy UE 2016/679 (GDPR) ed ogni provvedimento del Garante per la protezione dei dati personali e del WP Art. 29.

" **Appendice Security":** consiste nelle misure di sicurezza che il Titolare determina assicurando un livello minimo di sicurezza, e che possono essere aggiornate ed implementate dal Titolare, di volta in volta, in conformità alle previsioni del presente Accordo;

“ **Reclamo”:** si intende ogni azione, reclamo, segnalazione presentata nei confronti del Titolare o di un Suo Responsabile del trattamento;
“ **Titolare del Trattamento”:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
“ **Trattamento”:** 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;
“ **Responsabile del trattamento”** : la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento
“ **Pseudonimizzazione”** : il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Allegato 2

Appendice “Security”

L’ ASP deve adottare le misure minime per la sicurezza ICT stabilite da AGID con la circolare del 18 aprile 2017, n. 2/2017 pubblicata sulla Gazzetta Ufficiale, al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informativi.
Tali misure sono descritte all’indirizzo:
https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

Per ASP

_____

Per il fornitore

_____

Allegato 2 Policy aziendale sul "data breach"

Allegato 4 a deliberazione n. 2018/42 del 22/06/2018

POLICY GESTIONE INCIDENTI DI SICUREZZA

Sommario

1. Premessa

Il presente documento rappresenta il riferimento dell'Azienda Pubblica di Servizi alla Persona (ASP) "REGGIO EMILIA - Città delle persone" per la regolamentazione della gestione degli incidenti di sicurezza informatica che possano occorrere ai servizi e ai dati gestiti.

La corretta gestione degli incidenti di sicurezza permette di evitare o minimizzare la compromissione dei dati dell'organizzazione in caso di incidente; permette inoltre, attraverso l'analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell'incidente, di migliorare continuamente la capacità di risposta agli incidenti.

Inoltre, con specifico riferimento all'obbligo di cui all'art. 33 del GDPR n. 679/2016, il presente documento individua quali siano le violazioni che ricadono nell'ambito della suddetta normativa, i casi in cui ASP debba notificare i *data breach* all'Autorità Garante e agli interessati, le misure atte a trattare il rischio e la documentazione da produrre.

Si rappresenta che l'art. 32 del suddetto GDPR n. 679/2016 (di seguito Regolamento) dispone che devono essere approntate misure tecniche e organizzative adeguate per garantire un livello adeguato di sicurezza dei dati personali. Individuare, indirizzare e segnalare tempestivamente un incidente di sicurezza, come una violazione di dati, è espressione dell'adeguatezza delle misure implementate dall'Azienda.

L'ambito di applicazione è rappresentato da sistemi ICT di ASP e vengono presi in considerazione incidenti che possano scaturire sia dall'azione di un attacco informatico portato da elementi esterni

all’organizzazione, sia da un eventuale comportamento negligente o scorretto, di natura ostile con obiettivi frodatori da parte di uno o più collaboratori dell’Azienda.

Tutte le violazioni dei dati personali sono incidenti di sicurezza, ma non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.

L’obbligo di cui agli artt. 33 e 34 del Regolamento trova applicazione nei soli casi in cui la violazione riguardi dati personali, come definiti dall’art. 4 n. 1).

Il presente documento è applicabile alle risorse e ai servizi di tipo informatico gestiti in modo diretto oppure esternalizzato da parte di ASP “REGGIO EMILIA - Città delle persone”.

2. Incidente di sicurezza

Ai sensi del presente documento, per incidente di sicurezza deve intendersi “la violazione, la minaccia imminente di violazione di una politica di sicurezza informatica, di politiche di utilizzo accettabili o di prassi standard di sicurezza, correlate a una violazione di dati o informazioni”. Esempi di incidenti sono:

- un utente malintenzionato esegue operazioni al fine di inviare un numero elevato di richieste di connessione ad un server web, provocando l’arresto anomalo del servizio;
- gli utenti sono indotti ad aprire un file allegato alla mail che in realtà è un malware; l’esecuzione del tool che comporta l’infezione del dispositivo stabilendo connessioni con un host esterno;
- un utente malintenzionato ottiene dati sensibili e minaccia l’organizzazione di diffonderli se non viene pagato un riscatto in denaro.

3. Data breach ai sensi del GDPR

Il Regolamento definisce la violazione dei dati personali come “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”.

Le violazioni declinate dalla norma sono sintetizzabili come:

- **"Violazione della riservatezza"**, che si ha in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- **"Violazione dell'integrità"**, che si ha in caso di alterazione non autorizzata o accidentale dei dati personali;
- **"Violazione della disponibilità"**, che si ha in caso di perdita o distruzioni di dati personali o di impossibilità di accesso ai dati personali da parte di soggetti autorizzati.

Va sottolineato che una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione di queste.

Gli effetti di una violazione possono causare danni fisici, materiali o immateriali, ovverosia la perdita del controllo sui propri dati personali, la limitazione dei propri diritti, la discriminazione, il furto d'identità o la frode, la perdita finanziaria, l’ inversione non autorizzata di pseudonimizzazione, il danno alla reputazione e la perdita di riservatezza dei dati personali protetti dal segreto professionale. Può anche includere qualsiasi altro significativo svantaggio economico o sociale per gli individui che ne siano oggetto.

4. Notifica al Garante e agli interessati

In caso di *data breach* ASP valuta i rischi per i diritti e le libertà delle persone fisiche, registrando le evidenze di tale analisi.

Nell'eventualità che tale valutazione rappresenti elementi di rischio per i diritti e le libertà delle persone fisiche, l'Azienda effettua la notifica al Garante delle violazioni di dati personali.
Quando le violazioni di dati comportino un rischio valutato come elevato per i diritti e le libertà delle persone fisiche, devono essere comunicate agli interessati senza ingiustificato ritardo, fornendo loro specifiche informazioni in ordine alle salvaguardie che devono adottare per proteggere loro stessi dalle conseguenze della violazione.
Questo rischio esiste quando la violazione può comportare un danno fisico, materiale o immateriale per le persone i cui dati sono stati violati.; è presunto quando il *data breach* riguarda le categorie particolari di dati di cui all'art. 9 del Regolamento.
I criteri che devono guidare la valutazione del suddetto rischio sono i seguenti:
- la tipologia di violazione;
- la natura dei dati violati;
- il volume dei dati violati;
- il numero di individui cui si riferiscono i dati violati;
- caratteristiche speciali degli individui cui si riferiscono i dati violati;
- il grado di identificabilità delle persone;
- la gravità delle conseguenze per gli individui.

La valutazione viene condotta secondo una metodologia operativa adeguata, di seguito dettagliata.
ASP notifica la violazione dei dati personali all'autorità di controllo competente,senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui la medesima è stata rilevata. Oltre tale termine, tale notifica è corredata delle ragioni del ritardo e le informazioni sono fornite in fasi successive senza ulteriore ingiustificato ritardo.
Il termine decorre dal momento in cui l'Azienda ha consapevolezza della violazione di dati, ovverosia quando raggiunge un ragionevole grado di certezza che si è verificato un incidente di sicurezza che ha compromesso i dati personali dalla stessa trattati.
ASP può tardare la notifica all'Autorità Garante nei casi in cui la medesima possa produrre effetti negativi sugli individui interessati.
Nei casi in cui l'Azienda disponga di informazioni solo parziali della violazione, effettua comunque la notifica al Garante.
Il Garante per la protezione dei dati personali può richiedere, in ogni caso, la notifica della violazione agli interessati.
La comunicazione della violazione agli interessati può essere ritardata nei casi in cui tale comunicazione possa pregiudicare le indagini su cause, natura e conseguenze della violazione, anche su indicazione delle varie Autorità di controllo.
ASP utilizza lo strumento più efficace affinché tale comunicazione sortisca il maggiore effetto possibile.

5. Ruoli e responsabilità

La criticità del processo di gestione degli incidenti di sicurezza informatica e del *data breach* deve essere opportunamente affrontata da una struttura operativa competente, in possesso di adeguata formazione e in grado di prendere rapidamente le decisioni imposte dalla delicatezza del compito assegnato.
ASP istituisce a tal fine un **Gruppo per la Gestione della Sicurezza ICT**, adeguatamente dimensionato e strutturato con le seguenti competenze:

 rappresentare il punto di riferimento univoco a cui il personale dell'organizzazione deve rivolgersi per segnalare un potenziale incidente oppure un comportamento sospetto;
 gestire tutte le attività inerenti l'analisi e la gestione di un incidente di sicurezza, ivi comprese quelle relative alla sua notifica e documentazione;
 garantire la disponibilità delle liste di contatti (es.: personale dipendente, collaboratori, fornitori), necessarie per la gestione di un incidente di sicurezza;
 garantire che il processo di gestione incidenti sia sempre adeguato alle esigenze aziendali, provvedendo che il medesimo sia sempre aggiornato.

Il **Gruppo per la Gestione della Sicurezza ICT** è costituito dalle seguenti figure:
 Responsabile del Servizio Affari Generali e Giuridico legali con il ruolo di **Responsabile per la gestione della sicurezza ICT;**;
 Istruttore Direttivo Servizio Pianificazione e Controllo con il ruolo di **Referente per la gestione della sicurezza informatica**;
 Tecnico informatico.

I riferimenti del **Gruppo per la Gestione della Sicurezza ICT** (nominativi, indirizzo e-mail, numero di telefono ecc.) sono pubblicati sul sito istituzionale dell'Azienda nella sezione di Amministrazione trasparente "organizzazione/telefono e posta elettronica".
Nel corso del processo di gestione di un incidente di sicurezza informatico e, eventualmente, di un *data breach*, il Gruppo potrà essere coadiuvato di volta in volta dai Dirigenti cui fa capo il Servizio e/o la struttura i cui dati sono stati oggetto di *data breach* e da tutti coloro che il Gruppo stesso riterrà necessario coinvolgere, a seconda della tipologia di incidente e della tipologia di dati coinvolti.
Nelle attività del Gruppo deve essere coinvolto il *Data Protection Officer* (DPO) designato, il quale esercita le proprie funzioni di monitoraggio della conformità in caso di *data breach*, fornendo il proprio parere in ordine alla necessità di effettuare la notifica e, quindi, sulle valutazioni precedentemente descritte.
Il **Responsabile per la gestione della sicurezza ICT** ha il compito di attivare il Gruppo in caso di incidenti di sicurezza, di individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del DPO, e di segnalare al Titolare, in persona del Legale Rappresentante pro tempore, le violazioni dei dati personali ai fini della notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali.
Il Responsabile deve inoltre coinvolgere, a seconda della gravità dell'incidente, il Consiglio di Amministrazione, i Dirigenti e i Responsabili di Servizio dell'Azienda per gli aspetti di comunicazione interna ed esterna e, nel caso in cui, durante la gestione dell'incidente, emergano responsabilità da parte di personale interno, per gli eventuali provvedimenti disciplinari di competenza.
Nel caso in cui le attività di analisi dell'incidente di sicurezza evidenzino particolari difficoltà oppure impatti che si estendano al di fuori del perimetro aziendale, il Responsabile deve valutare l'opportunità o la necessità, di coinvolgere le strutture di riferimento regionali e nazionali (ad esempio, Lepida SpA, considerando il proprio ruolo nell'ambito della sicurezza della Community Network, CERT-PA, …). Inoltre, il Responsabile, oltre a coinvolgere i propri fornitori di servizi ICT per il supporto all'analisi e per l'ottenimento di informazioni utili, deve prevedere anche il coinvolgimento delle autorità di pubblica sicurezza, nel caso in cui l'incidente possa presentare risvolti dal punto di vista penale.
In caso di *data breach* il punto di contatto con il Garante per la protezione dei dati personali è costituito dal *Data protection officer*.

Il **Referente per la gestione della sicurezza informatica** è la figura che deve farsi carico della gestione di eventuali incidenti e cura che siano attivati comportamenti, attività e regolamenti per cercare di prevenire gli incidenti di sicurezza, riducendo il livello di rischio e l'esposizione a possibili attacchi informatici.

6. Procedura di gestione degli incidenti di sicurezza

ASP di seguito definisce la procedura per la gestione degli incidenti di sicurezza e ne garantisce il necessario aggiornamento. Tale procedura ha i seguenti obiettivi:

- preparare il personale;
- identificare un incidente in corso;
- minimizzare i danni relativi all'incidente e impedirne la propagazione;
- gestire correttamente il processo di ripristino dei sistemi e delle applicazioni;
- acquisire nel modo appropriato le eventuali evidenze digitali di reato;
- riconoscere gli errori commessi, assumerne le responsabilità e formulare proposte volte a migliorare la procedura stessa.

La decisione su quali soluzioni adottare è demandata al Gruppo di gestione della sicurezza ICT con l'eventuale supporto delle figure ritenute necessarie, tenendo conto della complessità e della variabilità dell'argomento trattato. Per facilitare la gestione degli incidenti di sicurezza ci si propone di rendere operativo un work flow che automatizzi le varie fasi, in particolare il flusso delle comunicazioni fra i vari attori. Tale misura potrà anche facilitare la produzione del report relativo all'incidente e potrà garantire di tenere aggiornate le statistiche sugli incidenti di sicurezza.

Nel caso si verifichi un incidente di sicurezza che possa pregiudicare per un periodo sufficientemente lungo la disponibilità delle informazioni occorrerà fare riferimento a disposizioni contenute in un piano di continuità operativa che l'Azienda adotterà con successivo atto con una chiara definizione delle strutture e delle responsabilità della gestione delle emergenze che dovranno operare in stretto coordinamento con il Gruppo di gestione della sicurezza.

Qualora, a seguito di un incidente relativo alla sicurezza delle informazioni, risulti necessario per ASP intraprendere un'azione legale (civile o penale) contro una persona fisica o giuridica, oppure nel caso in cui ci siano le premesse affinché l'Azienda possa essere oggetto di azione legale (civile o penale), le evidenze oggettive devono essere raccolte e conservate previo raccordo con il Responsabile del Servizio Affari Generali e Giuridico Legali, , e presentate in copia al medesimo Servizio, al fine di conformarsi ai requisiti di legge applicabili nelle sedi giurisdizionali competenti. Tutta la fase di raccolta delle evidenze deve essere fatta in modo che le evidenze siano utilizzabili in un processo giuridico. La raccolta delle evidenze può avvenire anche qualora si voglia semplicemente procedere con indagini più approfondite, non necessariamente legate ad un proseguo forense.

La documentazione relativa agli incidenti di sicurezza, comprensiva delle evidenze e delle valutazioni effettuate, viene elaborata in maniera tale da non indicare dati personali. Il tempo di conservazione di tale documentazione è stabilito in 24 mesi, nel caso in cui siano presenti dati personali, che, alla scadenza, devono essere cancellati e senza limiti di tempo, nel caso non siano presenti dati personali.

Tutti i dipendenti e collaboratori di ASP che accedono alle risorse del Sistema Informativo dell'Ente sono tenuti a osservare i principi contenuti nel presente documento e a segnalare in modo tempestivo la presenza di condizioni che possano indurre a valutare delle anomalie riconducibili ad attacchi informatici oppure a comportamenti scorretti.

Eventuali amministratori di sistema che, a causa del loro comportamento, gravemente negligente, o in palese contrasto con le politiche di sicurezza dell'Azienda, fossero causa diretta o indiretta di un

incidente di sicurezza, potranno essere soggetti a un accertamento di eventuali responsabilità rispetto alla violazione delle politiche di sicurezza ICT aziendali.

6.1 Identificazione e analisi dell'incidente

Tutti i potenziali incidenti di sicurezza di cui i dipendenti aziendali (utenti interni) siano a conoscenza, devono essere dagli stessi immediatamente comunicati, come primo punto di contatto, al Servizio Pianificazione e Controllo, la struttura organizzativa aziendale adibita alla gestione della sicurezza ICT.

Le segnalazioni di possibili incidenti di sicurezza devono pervenire via mail al **Referente per la gestione della sicurezza informatica** e, in sua assenza, al Responsabile del Servizio Pianificazione e Controllo.

Le segnalazioni possono arrivare al Referente, anche da alert automatici del sistema informativo aziendale, o da parte di utenti che, per esempio, possono rilevare situazioni di alterazione del sito web aziendale, di accesso non autorizzato a dati, di indisponibilità di una risorsa ICT per un tempo prolungato etc.

Nel caso di riscontro positivo di una segnalazione che pervenga in modo automatico dal processo di analisi continuativa degli eventi di sicurezza registrati da vari dispositivi, viene aperto un incidente di sicurezza che segue la procedura di gestione.

Nel caso di segnalazioni di incidente da parte di soggetti terzi, il Referente si attiva immediatamente per valutare se l'evento segnalato sia effettivamente riconducibile a un incidente di sicurezza, oppure si tratti di un cosiddetto falso positivo.

La notifica prevista dall'art. 33 del Regolamento viene effettuata al Garante a conclusione della verifica, qualora gli esiti della stessa consentano di appurare l'effettiva sussistenza della violazione.

a. VALUTAZIONE DELL'IMPATTO DELL'INCIDENTE

I possibili reali incidenti di sicurezza si possono classificare in diverse tipologie, dettagliate come segue: **Tipologia Incidente**	**Descrizione**
Accesso non autorizzato	Accesso (sia logico che fisico) a reti, sistemi, applicazioni, dati o altre risorse tecnologiche di proprietà dell'Ente da parte di personale non autorizzato.
Denial of Service	Attacco informatico alla disponibilità di una rete o sistema. Qualora abbia successo, comporta la difficoltà all'accesso o la totale indisponibilità di determinati sistemi e/o servizi.
Codice malevolo	Un virus, worm, trojan, spyware, o qualsiasi altro codice malevolo che infetti un sistema.
Uso Inappropriato	Violazione delle politiche di sicurezza e delle disposizioni su corretto utilizzo.
Data leakage	Diffusione di informazioni riservate a seguito di un attacco informatico riuscito.
Alterazione delle informazioni	Modifica del contenuto di dati riservati a seguito di un attacco informatico riuscito.