SERVIZIO DI ELABORAZIONE CENTRALIZZATA DEGLI STIPENDI DEL PERSONALE DI ASP REGGIO EMILIA CITTÀ DELLE PERSONE E ADEMPIMENTI CONNESSI PER IL PERIODO DI QUATTRO ANNI

CAPITOLATO SPECIALE

ART. 1 - OGGETTO DEL CONTRATTO

Il presente contratto ha come oggetto il servizio di elaborazione centralizzata degli stipendi del personale di ASP Reggio Emilia Città delle Persone ed adempimenti connessi

Per personale di ASP Reggio Emilia Città delle Persone si intende:

- Personale dipendente a tempo indeterminato ed a tempo determinato con applicazione del Contratto collettivo nazionale di Lavoro Comparto Funzioni Locali (circa n. 550 unità)
- Personale dipendente a tempo indeterminato ed a tempo determinato con applicazione del Contratto collettivo nazionale di Lavoro Area Funzioni Locali, ex Area II Regioni ed Autonomie Locali (circa n. 3 unità)
- Collaboratori coordinati e continuativi (circa n. 3 unità)

Tenuto conto della normativa vigente ed in particolare:

- Il contratto collettivo nazionale di lavoro relativo al personale del comparto funzioni locali del triennio 2019-2021 del 16.11.2022
- Legge n. 136/2023 coordinato ed aggiornato, da ultimo, con le modifiche apportate, da ultimo, dal D.L. 10 agosto 2023, n. 104, convertito, con modificazioni, dalla L. 9 ottobre 2023, n. 136**,** e dal D.L. 15 settembre 2023, n. 123, convertito, con modificazioni, dalla L. 13 novembre 2023, n. 159

ART. 2 - MODALITA' DI ESPLETAMENTO DEL SERVIZIO

Il servizio richiesto consta di un servizio base e di un servizio evoluto che comprende ed integra il precedente, comprendendo elaborazioni mensili e/o periodiche come di seguito esplicitato.

SERVIZIO BASE

a) Collegamento telematico all'applicativo residente presso ASP Reggio Emilia Città delle Persone
b) Foglio paga in formato elettronico
c) Riepilogo generale indicante i totali per voci contributive, i totali imponibili con relativi oneri per ogni singolo ente previdenziale, le ritenute fiscali ed il netto
d) Tracciato Setif per Tesoreria

e) Creazione file per invio telematico Uniemens/ DMA
f) denunce mensili INADEL-CPDEL-F.P.C. su quadro Z2
g) Elaborazione tredicesima mensilità entro i termini contrattuali
h) Lista imponibili e oneri fiscali/previdenziali per ciascun dipendente
i) Elaborazione Mod.770 parte personale
j) Elaborazione CU

SERVIZIO EVOLUTO (INCLUDE IL SERVIZIO BASE)

a) Invio del cedolino per la verifica a video
b) Foglio paga del dipendente in formato A4
c) Riepilogo generale indicante i totali per voci contributive, i totali imponibili con relativi oneri per ogni singolo ente previdenziale, le ritenute fiscali, ed il netto
d) Riepilogo per capitolo di spesa e/o costo (Contabilità da Agganci Contabili)
e) Distinta allegata al mandato in ordine alfabetico
f) Distinta allegata al mandato per capitolo di spesa e/o centro di costo
g) Tracciato setif/sepa per tesoreria, con raggruppamento distinto in base alla data di esecutività per dipendenti con conto presso istituto tesoriere (coincidente con la data di valuta degli stipendi mensili) o presso istituto diverso dal tesoriere (coincidente con la data antecedente la valuta degli stipendi mensili)
h) Creazione e controllo file per invio telematico UNIEMENS
i) Distinta contributi INADEL – CPDEL – F.P.C. per dipendente
j) Predisposizione modello F24 EP e creazione file per invio telematico, file unico comprensivo degli ambienti Dipendenti e Collaboratori
k) Denunce mensili INADEL – CPDEL – F.P.C. su quadro Z2
l) Controllo aggiuntivo, con eventuale consultazione del committente, su tutte le variazioni intervenute nel mese che incidono sulla DMA mensile
m) Invio per verifica a video e predisposizione DMA per invio telematico
n) Riepilogo voci utilizzate e relativi importi, totalizzati per capitolo di spesa
o) Stampa riepilogo IRAP, con specifica indicazione dell'IRAP di competenza in caso di dipendenti in comando parziale e per la tredicesima mensilità corrispondente alla durata del comando
p) Creazione file che generi il flusso di mandati e reversali (n. 3 files per stipendi, contributi e irap per ogni ambiente)

q) Personalizzazione delle voci retributive, capitoli d'imputazione, riferimenti sul cedolino di atti quali determinazioni e/o delibere

PERIODICAMENTE O SU RICHIESTA DI ASP REGGIO EMILIA CITTA' DELLE PERSONE VERRANNO FORNITE ANCHE LE SEGUENTI ELABORAZIONI:

a) Elaborazione tredicesima mensilità entro i termini contrattuali
b) Ricalcolo automatico di conguagli periodi pregressi, relativi a variazioni fisse o tabellari, nonché dei corrispondenti figurativi per assenze per maternità o per malattia del figlio, previo invio dei relativi dati (per rinnovo CCNL o accordi aziendali)
c) Lista imponibili e oneri fiscali/previdenziali per ciascun dipendente
d) Stampa del modello CU anticipato per dipendenti cessati in corso d'anno, entro 12 giorni dalla richiesta del dipendente
e) Stampe inerenti ai centri di costo
f) Possibilità di estrapolazione/trasmissione di dati per il "controllo di gestione"
g) Circolari con modifiche software riferite alla normativa vigente nel periodo
h) Conto annuale tabelle 12, 13 e parzialmente 14 con i dati gestiti dai Programmi in essere
i) Prospetto denuncia annuale IRAP
j) Elaborazione e controllo modello 770
k) Denuncia 770 (tutti i quadri) su modulo ministeriale in formato pdf
l) Denuncia 770 (tutti i quadri) in formato telematico ministeriale
m) Invio telematico del modello 770 tramite intermediario abilitato
n) Stampa modello CU Stampa per denuncia annuale INAIL
o) Stampa bilancio di previsione costo del personale
p) Ulteriori adempimenti obbligatori per legge
q) Conteggio autoliquidazione premio INAIL

ART. 3 - SOLUZIONI TECNICHE ED ORGANIZZATIVE PER L'ESPLETAMENTO DEL SERVIZIO

Per tutta la durata del servizio, l'Appaltatore utilizzerà l'applicativo "**Job Time Stipendi**" o altro applicativo installato presso il server del committente, assistito, a latere, da specifico contratto di manutenzione che ne regola anche le modalità ed i limiti di utilizzo.

Per l'attività oggetto del presente contratto saranno concordate le modalità di attivazione del collegamento dalla sede dell'Appaltatore, nel rispetto delle specifiche tecniche, delle norme in materia e delle misure per la protezione dei dati personali.
Sarà altresì approntata sul medesimo server una Cartella condivisa da utilizzarsi per il deposito dei files di input e di output del processo di elaborazione stipendi.
Appaltatore e committente utilizzeranno inoltre strumenti quali e-mail e/o comunicazioni telefoniche esclusivamente per i raffronti operativi, i riscontri e la validazione delle diverse fasi del processo, le autorizzazioni alla chiusura delle elaborazioni, escludendo l'utilizzo per trasmissione/elaborazione dati.

ART. 4 - CARICAMENTO DEI DATI

Il Committente provvederà ogni mese al caricamento sull'applicativo Job Time Stipendi installato presso il proprio server dei dati anagrafici, retributivi e fiscali dei dipendenti in forza e delle variazioni avvenute nel periodo.
Tali caricamenti saranno effettuati nel rispetto dei tempi di seguito indicati, in tempo utile per consentire l'elaborazione dei dati e la consegna da parte dell'Appaltatore di tutti i prospetti sopra indicati.
In considerazione della natura dei dati trattati e della modalità condivisa di utilizzo/accesso all'applicativo Job Time Stipendi, il servizio prevede una traccia di registrazione (log) di tutte le operazioni di modifica, secondo quanto previsto dalla normativa. Tale registro delle operazioni effettuate è immodificabile da chiunque ed è accessibile ai responsabili autorizzati. Anche tali eventuali accessi, sono registrati in modo certo.

ART. 5 - CALENDARIO DEGLI ADEMPIMENTI

Il Committente provvederà all'inserimento delle variabili entro il 15 di ogni mese, con anticipo se coincidente con la chiusura degli uffici amministrativi. Sono fatti salvi gli inserimenti urgenti pervenuti dopo tale data da concludersi comunque entro e non oltre il 18 di ogni mese
L'Appaltatore predisporrà l'elaborazione degli stipendi e provvederà alla relativa chiusura, previo accordo con il Committente, entro e non oltre il 21 di ogni mese, con anticipo se coincidente con la chiusura degli uffici amministrativi.
La valuta degli stipendi sarà il 27 di ogni mese, qualora il 27 fosse coincidente con il sabato o con la domenica, la valuta dovrà essere anticipata rispettivamente al 26 o al 25 del mese.
La data fissata per gli stipendi del mese di dicembre unitamente alla tredicesima mensilità è il 18 dicembre .

L’Appaltatore provvederà alla stampa del cedolino WEB sul portale del Committente il giorno antecedente la valuta di pagamento degli stipendi mensili

ART. 6 - ASSISTENZA TECNICA

L’Appaltatore mette a disposizione del Committente la propria struttura tecnica per supportare, attraverso l’assistenza telefonica e telematica, gli operatori su tutte le problematiche di tipo informatico, funzionale e sulla materia specifica del personale. Attraverso numeri dedicati il Committente potrà accedere al servizio desiderato confrontandosi direttamente con la persona.

Gli orari di copertura del servizio sono i seguenti dal lunedì al venerdì dalle 08.30 alle 13.30 e dalle 14.00 alle 18.00, il Committente potrà inoltre, previa prenotazione, ricevere assistenza normativa, fiscale e previdenziale, direttamente dal coordinatore del servizio o da persona da esso delegata. Per problemi urgenti il Committente avrà inoltre a disposizione n. 3 numeri di telefoni cellulare che potrà contattare per richieste urgenti. Attraverso il sito aziendale dell’Appaltatore viene garantito un servizio dedicato cui il Committente può accedere autonomamente in qualsiasi momento digitando i codici assegnati. All’interno dell’area ad accesso riservato del sito il Committente potrà reperire le informazioni che Appaltatore renderà quotidianamente disponibili sulla normativa, sulle novità ultime introdotte dal legislatore, sullo stato del software in utilizzo, sulle personalizzazioni che lo riguardano, sullo stato delle richieste da esso effettuate, nonché su tutta una serie di altri servizi di estrema utilità.

Per tutta la durata del contratto l’Appaltatore si impegna a fornire i servizi di assistenza tecnica necessari ad assicurare il corretto funzionamento e utilizzo delle procedure. In particolare durante l’orario di apertura dell’ufficio del Committente, garantirà:

- l’assistenza di proprio personale raggiungibile tramite assistenza telefonica e telematica;
- la consulenza ed il supporto per il miglior utilizzo del software applicativo
- il corretto recepimento da parte del personale dell’ente delle modalità operative e dei servizi erogati
- la collaborazione per la soluzione di problemi pratici di natura tecnica, giuridica, contrattuale;
- il buon funzionamento del software messo a disposizione per la durata contrattuale assumendosi l’obbligo di eliminare eventuali anomalie e/o malfunzionamenti.

Il Committente informerà prontamente l’Appaltatore di ogni malfunzionamento e/o delle anomalie che si verifichino, specificando le caratteristiche del problema; l’Appaltatore garantirà il ripristino delle funzionalità entro un massimo di 24 ore dalla segnalazione pervenuta.

ART. 7 - CONSULENZA

Compreso nel servizio di elaborazione degli stipendi è previsto un aggiornamento, redatto da Consulente del Lavoro abilitato con regolare contratto in essere con l'Appaltatore, attraverso l'invio di lettere informative allo scopo di rendere edotti gli operatori sulle principali novità in materia fiscale e del lavoro in genere.

Punto di ascolto (front-office)

La continua evoluzione delle normative fiscali e del lavoro necessitano di una presenza pressoché costante di professionisti esperti del settore che, attraverso consulenze mirate e con l'apporto di adeguata documentazione, permettano all'Ente di essere costantemente informato. Da ciò l'idea di creare il cosiddetto "Punto di ascolto" che sarà organizzato come segue: quotidianamente attraverso la risoluzione e/o l'interpretazione di problemi mediante interrogazioni e risposte via e-mail "Punto di ascolto virtuale".

ART. 8 - CORRISPETTIVO E CONDIZIONI DI PAGAMENTO

Il servizio di elaborazione degli stipendi come sopra indicato e descritto, comprensivo del servizio base e del servizio evoluto e comprensivo delle elaborazioni periodiche obbligatorie o a richiesta sopra indicate ai punti . 2,3,4,5,6,7 viene fornito dietro corrispettivo unitario di

€ …… (come da vostra offerta) + IVA per ogni cedolino stipendiale mensile elaborato

La tredicesima verrà fatturata come elaborazione aggiuntiva anche se incorporata nella mensilità di dicembre.

In applicazione del meccanismo di assolvimento dell'IVA c.d. "split payment", introdotto dall'art. 1 commi 629 – 633 della legge 190/2014 (Legge di stabilità 2015), l'ASP pagherà all'appaltatore l'imponibile e tratterrà l'IVA che provvederà successivamente a versare all'Erario. L'Appaltatore dovrà emettere fattura secondo quanto previsto dall'art. 21 D.P.R. n. 633/1972 con l'annotazione "scissione dei pagamenti", registrare la fattura emessa ai sensi degli artt. 23 e 24 del D.P.R. n. 633/1972 senza computare l'IVA in essa indicata nella liquidazione periodica.

L'appaltatore si impegna ad assumere tutti gli obblighi di tracciabilità dei flussi finanziari ai sensi di quanto disposto dalla L. 136/2010 sue m. e i., il pagamento verrà eseguito esclusivamente a mezzo bonifico sul conto corrente bancario dedicato.

Prima dei singoli pagamenti, verrà verificata da parte dell'Azienda la regolarità del DURC: nel caso si verifichi una situazione di DURC non regolare, si procederà ai sensi della vigente normativa in caso di inadempienza contributiva.

A norma dell'art. 11 comma 6 del Decreto legislativo 36/2023 sull'importo netto delle prestazioni fatturate sarà operata una ritenuta dell'0,5%, a garanzia dell'adempimento da parte dell'Appaltatore delle norme dei contratti collettivi di lavoro, delle leggi e dei regolamenti sulla tutela, sicurezza, assicurazione ed assistenza dei lavoratori. Tali somme saranno svincolate in sede di pagamento finale, dopo l'approvazione del certificato di regolare esecuzione, previo rilascio del DURC.

L'Azienda non rifonde inoltre le spese per commissioni bancarie, né per bolli applicati sulla fattura che sono a carico dell'aggiudicatario. In base all'art. 1 commi 209 – 2014 della Legge 244/2007 e al Decreto Ministeriale n. 55/2013, l'emissione, la trasmissione, la conservazione e l'archiviazione delle fatture emesse nei rapporti con la Pubblica Amministrazione deve essere effettuata esclusivamente in forma elettronica. In ottemperanza al citato Decreto dal 31 marzo 2015 le fatture dovranno essere trasmesse in forma elettronica, secondo il formato di cui all'Allegato A del citato DM 55/2013.
La fattura che dovrà essere emessa conformemente all'Allegato B "Regole Tecniche" del DM 55/2013 e trasmessa per mezzo del Sistema di Interscambio, dovrà obbligatoriamente riportare oltre al CIG indicato sul contratto il seguente Codice Univoco Ufficio: UFZ0Y9.
In mancanza di tali elementi nella fattura elettronica, Asp non potrà procedere al pagamento della fattura stessa.

ART. 9 - SERVIZI AGGIUNTIVI

In aggiunta al servizio come sopra indicato, l'Appaltatore si obbliga a fornire, su specifica richiesta del committente, i servizi di seguito indicati alle condizioni economiche successivamente previste

A) Invio telematico Certificazioni Uniche (CU) riferite ai lavoratori DIPENDENTI

L'invio telematico avrà un costo, per annualità, pari a:

Fascia 3 > 50 percipienti **Euro ……(come da vostra offerta) + IVA/anno**

B) Ricezione in via telematica dei dati relativi ai mod. 730-4

Il servizio prevede la ricezione, da parte dell'Agenzia delle Entrate, previo invio del modello previsto, del risultato contabile delle dichiarazioni. Attraverso un consulente abilitato, si assicura il monitoraggio costante dei risultati dei mod. 730 inviati e le conseguenti eventuali variazioni da apportare.

Euro……(come da vostra offerta) + IVA/anno

ART. 10 - REVISIONE PREZZI

Qualora nel corso di esecuzione del contratto, al verificarsi di particolari condizioni di natura oggettiva, si determini una variazione, in aumento o in diminuzione, del costo del servizio e/o dei beni superiore al cinque per cento, dell'importo complessivo, i prezzi sono aggiornati, nella misura dell'ottanta per cento della variazione, in relazione alle prestazioni da eseguire. Ai fini del calcolo della variazione dei prezzi si utilizzano gli indici ISTAT –FOI esclusi i tabacchi. La revisione dei prezzi deve avere le seguenti caratteristiche:

1. non deve apportare modifiche sostanziali al contratto;
2. si applica al verificarsi di particolari condizioni di natura oggettiva, che determinano una variazione del costo della prestazione in più o meno superiore al 5% dell'importo complessivo dell'intervento, da determinarsi in base agli indici sintetici delle variazioni dei costi e dei prezzi dei lavori, servizi e forniture, approvati dall'Istat entro il 30 settembre di ogni anno;
3. copre la variazione nella misura dell'80% della stessa.

Le clausole revisionali non attribuiscono all'appaltatore un diritto alla revisione dei prezzi, ma l'interesse legittimo all'apertura di un procedimento tecnico discrezionale da parte dell'Azienda, che deve valutare la sussistenza dei presupposti di legge per il suo riconoscimento.

Asp potrà inoltre variare sino a concorrenza del quinto dell'importo del contratto.

ART. 11 - CLAUSOLA DI RINEGOZIAZIONE

Ai sensi dell'articolo 9 del Codice, la stazione appaltante, poiché il contratto risulta particolarmente esposto per la sua durata, per il contesto economico di riferimento o per altre circostanze, al rischio delle interferenze da sopravvenienze, prevede clausole di rinegoziazione al verificarsi delle indicate condizioni la cui sussistenza dovrà essere dimostrata dalla parte svantaggiata:

1. non aver assunto volontariamente il rischio dell'evento sopravvenuto;
2. l'avvenimento sopravvenuto derivi da eventi straordinari e imprevedibili (inimmaginabili al momento della stipula);
3. estraneità delle sopravvenienze all'alea contrattuale e alle normali fluttuazioni di mercato.

La presentazione della domanda di rinegoziazione non comporta automaticamente la sospensione dell'esecuzione del contratto che, come prevede l'art. 121 (sospensione dell'esecuzione) del d.lgs. 36/2023, va valutata dall'Azienda.

Il compito di istruire la pratica e provare a trovare un accordo spetta al Responsabile Unico di Progetto entro un termine non superiore a tre mesi.

Le parti *devono adottare comportamenti adeguati alle concrete circostanze, allo specifico contenuto contrattuale e alla qualificazione dei soggetti interessati, con proposte serie e sostenibili, che potranno investire tutti i contenuti del contratto: modalità della prestazione, tollerandone variazioni, durata, prezzo, ecc. L'utilizzo della clausola impone alle parti l'individuazione della concreta regola di condotta corrispondente alla buona fede con riferimento al caso specifico, in linea con la nuova fiducia riposta nei contraenti e la valorizzazione dell'autonomia decisionale dei funzionari pubblici di cui all'art. 2 "Principio di fiducia"*.

L'accordo raggiunto tra le parti dà vita a un nuovo contratto che si sostituisce a quello originario e che deve, pertanto, essere sottoscritto dal dirigente o responsabile del servizio. Nel caso in cui le parti non pervengano a un accordo entro un termine ragionevole, da valutarsi in base alle circostanze specifiche, la parte svantaggiata potrà rivolgersi al giudice per ottenere l'adeguamento del contratto all'equilibrio originario, fatta salva la responsabilità della parte inadempiente all'obbligo di rinegoziare in buona fede.

L'attività di rinegoziazione è sottoposta ai seguenti limiti:

1. il divieto di snaturare il contratto, apportandovi modifiche tali da far ritenere la stipula di uno nuovo;
2. il ripristino dell'originario equilibrio del contratto e della sua sostanza economica, in considerazione degli atti della gara;
3. il riconoscimento dei maggiori compensi all'appaltatore a valere sulle somme a disposizione nel quadro economico dell'intervento, alla voce imprevisti e accantonamenti e, se necessario, anche utilizzando le economie da ribasso d'asta (obbligo di invarianza finanziaria), che, poiché possono considerarsi definitivamente acquisite solo al momento della verifica di conformità, vanno utilizzate previa attenta valutazione *in relazione al caso concreto (es. con riferimento allo stato di avanzamento dell'opera) e sulla base di adeguata motivazione*;
4. *forme del procedimento amministrativo, che ne consente il controllo da parte degli altri operatori economici e del giudice poiché il contratto pubblico non consente modifiche sostanziali al fine di non ledere il principio della concorrenza*.

ART. 12 - RESPONSABILE UNICO DEL PROGETTO E DIRETTORE DELL'ESECUZIONE CONTRATTUALE

Il servizio in oggetto è considerato, conformemente a quanto disposto dall'art. 32, comma 2, dell'allegato II.14, capo II, del d.lgs. 36/2023, di particolare importanza, indipendentemente dall'importo, per ragioni sia attinenti alle prestazioni – che richiedono l'apporto di una pluralità

di competenze – sia concernenti l'organizzazione interna alla stazione appaltante, in quanto impongono il coinvolgimento di un'unità organizzativa diversa da quella a cui afferiscono i soggetti che hanno curato l'affidamento.

Il Responsabile Unico del Progetto (RUP) è il Dirigente dell'Area Risorse Umane e Finanziarie, dott. Teodoro Vetrugno che svolge anche i compiti e le attività del direttore delle esecuzioni contrattuali (DEC). Al RUP sono attribuiti i compiti di cui all'allegato I.2 del d.lgs. 36/2023, a cui si fa rinvio.

Il RUP/DEC individua nella responsabile del Servizio Politiche del Personale dott.ssa Marika Franco il direttore Operativo

ART. 13 - OBBLIGHI DELL'APPALTATORE – SICUREZZA – SEGRETO D'UFFICIO – TRATTAMENTO DEI DATI

L'Appaltatore si impegna a svolgere l'attività prevista dal presente contratto attuando tutte le misure di sicurezza anche verso terzi secondo le regole dell'arte.

L'Appaltatore si obbliga al rispetto di quanto previsto dal D.Lgs. 81/2008 tutti i lavoratori chiamati ad operare presso il Committente dovranno essere adeguatamente formati ed informati in materia di sicurezza sui luoghi di lavoro, più precisamente formati ed informati sull'utilizzo delle attrezzature/impianti, sull'impiego dei dispositivi di protezione individuali, quindi essere correttamente formati ed informati sui rischi presenti sul luogo di lavoro. Le parti si impegnano a cooperare per attuare tutte le misure necessarie di prevenzione e protezione rischi sul lavoro relative all'attuazione del presente servizio.

Nei confronti dei propri lavoratori l'Appaltatore dovrà:

- osservare tutte le leggi i regolamenti, i contratti di categoria in vigore ed ogni altra disposizione in materia di rapporto di lavoro, ivi compresa ogni disposizione in materia di sicurezza e protezione dei lavoratori medesimi come sopra indicato;
- corrispondere correttamente tutti gli oneri previdenziali, assicurativi ed assistenziali dovuti, oltre ogni altro adempimento inerente il rapporto di lavoro;

L'Appaltatore sarà tenuta ad esibire in qualunque momento ed a semplice richiesta della committente, documentazione idonea a provare la propria regolarità nei confronti degli obblighi verso i lavoratori e verso le disposizioni vigenti in materia assicurativa.

L'Appaltatore si impegna a osservare e fare osservare al personale impiegato, per quanto compatibili con l'attività svolta, 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 di ASP REGGIO EMILIA Città delle persone, approvato con deliberazione del C.d.A. n. 2016/30 del 12.04.2016 .

A tal fine 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 .

L'Appaltatore 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 del committente.

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.

L'Appaltatore 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 della Committente per eventuali violazioni dell'obbligo di riservatezza commesse dai suddetti soggetti.

L'Appaltatore può utilizzare servizi di cloud pubblici ove memorizzare i dati e le informazioni trattate nell'espletamento dell'incarico affidato, solo previa autorizzazione del committente.

In caso di inosservanza degli obblighi descritti nei punti precedenti, il committente ha facoltà di dichiarare risolto di diritto il Contratto, fermo restando che l'appaltatore sarà tenuto a risarcire tutti i danni che ne dovessero derivare. L'Appaltatore potrà citare i termini essenziali del Contratto nei casi in cui fosse condizione necessaria per la partecipazione del 'Appaltatore stesso a gare e appalti, previa comunicazione al committente delle modalità e dei contenuti di detta citazione.

Sarà possibile ogni operazione di auditing da parte del committente attinente le procedure adottate dall'appaltatore 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. L'appaltatore 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.

L’appaltatore 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 l’appaltatore "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 l’appaltatore 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, l’appaltatore sarà considerato responsabile nei confronti del Titolare ai sensi di legge. In caso l’appaltatore 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, l’Appaltatore, 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)

ART. 14 - ULTERIORI OBBLIGHI DELL’AFFIDATARIO

L'affidatario è tenuto a comunicare tempestivamente alla committente ogni modificazione intervenuta negli assetti proprietari e nella struttura di impresa, nonchè negli organismi tecnici e amministrativi, relativi anche alle imprese affidatarie del subappalto.

L’affidatario si assume, inoltre, l’onere di comunicare ogni variazione dei requisiti ai sensi dell’articolo 96 comma 12 d.lgs. 36/2023.

ART. 15 – CESSIONE E SUBAPPALTO

Fatto salvo quanto previsto dall’articolo 120, c. 1, lett. d), la cessione del contratto è nulla. L’appaltatore può cedere i crediti derivanti dal contratto con le modalità espresse all’art. 120 comma 12 del Codice. Alle cessioni di crediti si applicano le disposizioni di cui alla L. n. 52/1991 e quanto previsto dall’allegato II.14 – articolo 6 Cessioni di crediti.

E’ ammesso il subappalto nel rispetto di limiti e nel rispetto delle modalità indicate all’art. 119 del D.lgs. 36/2023.

Il subappaltore è soggetto agli stessi obblighi dell'appaltatore in tema di protezione dei dati personali e particolari ai sensi del Regolamento Europeo 679/2016.

L’ASP non individua prestazioni contrattuali che debbano necessariamente essere eseguite dall’affidatario.

ART. 16 - GARANZIE

A titolo di garanzia definitiva l'Appaltatore sarà tenuto a presentare, a sua scelta sotto forma di cauzione o fideiussione con le modalità previste dall’articolo 53 comma 4 del codice.

ART. 17 - INADEMPIENZE – PENALI

L’Appaltatore assumerà ogni responsabilità in caso di danni eventualmente arrecati a persone o cose nella realizzazione del servizio, in tal caso si impegna sin d’ora al totale risarcimento degli eventuali danni causati a terzi, esonerando il committente da ogni responsabilità.

In particolare per inadempimenti nella elaborazione, consegna, trasmissione di quanto previsto all'art. 2 sono previste penali in misura:

- l'1 per mille dell'ammontare netto contrattuale per ogni giorno di ritardo nei casi di inadempimenti accertati rispetto alla predisposizione di elaborazioni previste all'art. 2 con scadenze definite.

- sino a un massimo del 10% dell'ammontare netto contrattuale in caso di mancato adempimento, interruzioni della continuità del servizio non dovute a cause di forza maggiore e altre violazioni gravi.

La comminazione della penale, in ogni caso, non impedisce il risarcimento del maggior danno.

L'affidatario è responsabile anche per gli eventuali inadempimenti (totali o parziali) dovuti a soggetti terzi coinvolti dallo stesso nell'esecuzione dell'appalto.

L'Azienda potrà compensare i crediti derivanti dall'applicazione delle penali di cui al presente articolo con quanto dovuto all'affidatario a qualsiasi titolo, ovvero avvalersi della garanzia senza bisogno di diffida, ulteriore accertamento o procedimento giudiziario. La richiesta e/o il pagamento delle penali di cui al presente articolo non esonera in nessun caso l'affidatario del servizio dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere l'obbligo di pagamento della medesima penale.

Relativamente alle contestazioni in corso di esecuzione, il RUP, prima di applicare le penali, procederà alla regolare contestazione scritta dell'inadempienza avverso la quale la ditta avrà facoltà di presentare le sue controdeduzioni entro 3 (tre) giorni dal ricevimento della contestazione stessa. Resta, in ogni caso, ferma la facoltà della Stazione Appaltante, in caso di gravi violazioni, di sospendere immediatamente il servizio alla ditta appaltatrice e di affidarla anche provvisoriamente ad altra ditta, con costi a carico della parte inadempiente e immediata escussione della garanzia definitiva. Il pagamento della penale dovrà essere effettuato entro 15 (quindici) giorni dalla notifica o dalla ricezione della comunicazione di applicazione. Decorso tale termine la Stazione Appaltante si rivarrà trattenendo la penale sul corrispettivo della prima fattura utile con emissione di nota di credito, ovvero sulla garanzia definitiva. In tale ultimo caso la ditta è tenuta a ripristinare il deposito cauzionale entro 10 (dieci) giorni dalla comunicazione del suo utilizzo pena la risoluzione del contratto.

Tutte le penalità potranno essere tra loro cumulabili a seconda del tipo di inadempienza contestata. In ogni caso di inadempimento, o di mancato rispetto delle condizioni stabilite, la stazione appaltante invierà comunicazione scritta con specifica motivata delle contestazioni, con richiesta di giustificazioni (che dovranno pervenire alla Stazione Appaltante entro 5 giorni dal ricevimento della

contestazione) e con invito a conformarsi immediatamente alle prescrizioni del presente capitolato. Nel caso in cui le giustificazioni addotte non fossero ritenute accoglibili dalla stazione appaltante, o in caso di mancata risposta o di mancato arrivo nel termine indicato, si procederà all'applicazione delle penali.

Trattandosi di servizio con prestazioni continuative, sono previste verifiche di conformità in corso di esecuzione contrattuale, al fine di accertare la piena e corretta esecuzione delle prestazioni, con accertamenti progressivi di cadenza annuale, ritenuta adeguata alla complessità e all'entità del servizio. Della data di effettuazione delle verifiche il DEC deve dare comunicazione all'esecutore affinché quest'ultimo possa intervenire in contraddittorio.

Detti controlli saranno effettuati in contraddittorio tra le parti. Nel caso in cui il responsabile del servizio non fosse presente per il contraddittorio, l'ente o i suoi incaricati effettuerà ugualmente i controlli e il Fornitore non potrà contestare le risultanze di detti controlli.

Resta peraltro salva la facoltà di eseguire verifiche a sorpresa.

Gli organismi incaricati dalla singola amministrazione contraente effettueranno i controlli secondo la metodologia che riterranno più idonea.

Qualora sia ritenuto opportuno in sede di esecuzione contrattuale, il RUP/DEC può impartire all'esecutore le disposizioni e le istruzioni necessarie tramite ordini di servizio, che devono riportare le motivazioni alla base dell'ordine. Gli ordini di servizio devono avere forma scritta e l'impresa affidataria deve restituire gli ordini stessi firmati per avvenuta conoscenza, fatte salve eventuali contestazioni. Per tutto quanto qui non previsto, anche con riferimento alle contestazioni e riserve, alla valutazione delle variazioni contrattuali nonchè alla regolare esecuzione e relativa certificazione, si rinvia agli artt. 114 e 115 del d.lgs. 36/2023 nonchè all'allegato II.14, capo II, del decreto legislativo stesso.

ART. 18 - RESPONSABILITÀ VERSO TERZI

L'Appaltatore del servizio oggetto del presente appalto, si obbliga a stipulare con primario assicuratore (e mantenere in vigore per tutta la durata del presente contratto, suoi rinnovi e proroghe) una polizza di assicurazione di Responsabilità Civile verso Terzi (RCT/RCO), con effetto dalla data di decorrenza del servizio, per danni arrecati a terzi in conseguenza di un fatto verificatosi in relazione all'attività svolta, comprese tutte le operazioni di attività inerenti, accessorie e complementari, nessuna esclusa nè eccettuata con massimali non inferiori a:

- € 1.000.000,00 unico per la garanzia RCT
- € 1.000.000,00 per sinistro, con sottolimite di € 500.000,00 per persona per la garanzia RCO

e che preveda, tra le altre condizioni, anche:

a) la Responsabilità Civile derivante da fatto (anche doloso) di persone della cui opera il fornitore si avvalga (dipendenti e non);
b) (chiedere se svolge la propria attività c/o i locali della Stazione appaltante) estensione alla RC derivante dalla conduzione e gestione dei locali, dai danni alle cose in consegna o custodia, dai danni a cose di terzi da incendio di beni del fornitore o da lui detenuti;
c) estensione nel novero dei terzi alle persone che prestano la loro collaborazione per lo svolgimento dell'attività del fornitore nell'ambito dei locali e degli spazi in genere concessi in sub-concessione.
Le coperture assicurative stipulate dal fornitore del servizio dovranno essere mantenute in essere fino al termine del contratto e di sue eventuali proroghe.
ASP sarà in ogni caso tenuta indenne dai danni eventualmente non coperti in tutto o in parte dalle polizze assicurative del fornitore.
L'operatività o meno delle coperture assicurative non esonera il fornitore dalle responsabilità di qualunque genere su di esso incombenti.
Dovrà inoltre essere prevista la rinuncia all'azione di rivalsa nei confronti ASP per qualsiasi danno, infortunio o altro evento dannoso cagionato sia a Terzi che al personale dipendente del fornitore, durante lo svolgimento del servizio. ASP sarà sollevata ed indenne da qualsivoglia danno, diretto ed indiretto, derivante dall'attività oggetto dell'appalto e rimangono pertanto esentate da ogni azione, giudiziale o stragiudiziale, da chiunque instaurata.
ASP dovrà inoltre essere inserita nel novero dei Terzi.
Il fornitore del servizio oggetto del presente appalto, si obbliga altresì a stipulare con primario assicuratore (e mantenere in vigore per tutta la durata del presente contratto, suoi rinnovi e proroghe) una polizza di assicurazione di Responsabilità Civile Professionale, con effetto dalla data di decorrenza del servizio, per errori e/od omissioni in relazione all'attività svolta, comprese tutte le operazioni di attività inerenti, accessorie e complementari, nessuna esclusa nè eccettuata con massimali non inferiori a:

- € 1.000.000,00 per sinistro.

ART. 19 - RISOLUZIONE DEL CONTRATTO

Per la risoluzione del contratto trovano applicazione l'art. 122 del D.Lgs. 36/2023 e all'art. 10 dell'Allegato II.14 del D.lgs. 36/2023, nonché gli articoli 1453 e ss. del Codice Civile.
Il contratto si risolve di diritto, ai sensi dell'articolo 1456 del Codice Civile, con la semplice comunicazione da parte della committente all'affidatario di volersi avvalere della clausola risolutiva

espressa, qualora l'affidatario non adempia agli obblighi di tracciabilità dei movimenti finanziari relativi al presente contratto ai sensi dell'articolo 3, comma 9bis della legge n. 136/2010.
Ai sensi e per gli effetti dell'art. 1 comma 13 del D.L. n. 95/2012 convertito con modificazioni nella Legge 7 agosto 2012, n. 135, l'Azienda ha diritto di recedere in qualsiasi momento dal presente contratto nel caso in cui sopravvengano convenzioni CONSIP o Intercent-ER migliorative rispetto a quelle del presente contratto, secondo le modalità di cui al medesimo art. 1 comma 13 D.L. n. 95/2012 convertito con modificazioni nella Legge 7 agosto 2012, n. 135.

ART. 20 - RECESSO DAL CONTRATTO

La committente può recedere dal contratto, in qualunque tempo e fino al termine della prestazione, secondo la procedura prevista dall'articolo articolo 123 del d.lgs. 36/2023 e dell'art. 11 dell'Allegato II.14 del d.lgs. 36/2023. Tale facoltà è esercitata dall'Azienda con preavviso di almeno trenta giorni, da comunicarsi all'appaltatore con PEC. Dalla data di efficacia del recesso, l'appaltatore dovrà cessare tutte le prestazioni contrattuali, assicurando che tale cessazione non comporti danno alcuno all'Azienda. In caso di recesso dell'Azienda, l'appaltatore ha diritto al pagamento di quanto correttamente eseguito a regola d'arte, oltre al decimo dell'importo dei servizi non eseguiti. Tale decimo è calcolato sulla differenza tra l'importo dei quattro quinti del prezzo posto a base dell'affidamento, depurato della migliore proposta fatta dall'appaltatore e l'ammontare netto delle prestazioni eseguite. Si applica in ogni caso quanto previsto dall'art. 123 del Codice.
In caso di sopravvenienze normative interessanti l'Azienda che abbiano incidenza sull'esecuzione del servizio, la stessa potrà recedere per giusta causa in tutto o in parte unilateralmente dal contratto, con un preavviso di almeno trenta giorni da comunicarsi all'appaltatore con PEC. Nelle ipotesi di recesso per giusta causa, l'appaltatore ha diritto al pagamento di quanto correttamente eseguito a regola d'arte secondo i corrispettivi e le condizioni di contratto e rinuncia, ora per allora, a qualsiasi pretesa risarcitoria, a ogni ulteriore compenso o indennizzo e/o rimborso delle spese, anche in deroga a quanto stabilito all'art. 1671 Codice Civile.

ART. 21 – CONTROVERSIE E FORO COMPETENTE

Tutte le controversie che dovessero insorgere relativamente al rispetto delle clausole e condizioni del presente contratto e che non si siano potute definire in via amministrativa, saranno devolute alla autorità giudiziaria ordinaria, con esclusione della competenza arbitrale. Il Foro competente in via esclusiva, ai sensi dell'art. 25 del Codice di Procedura Civile, è quello di Reggio Emilia. Si applicano, nel caso di controversie di importo economico non inferiore al 10% dell'importo di

contratto, le disposizioni di cui agli artt. 210 e 211 del D.Lgs 36/2023. L'imposta sul valore aggiunto è regolata come per legge.

ART. 22 - DURATA DEL CONTRATTO

Ferma restando l'eventuale esecuzione anticipata di cui all'art. 17, comma 8, del D.Lgs.36/2023, la durata dell'appalto è di 48 mesi, decorrenti indicativamente dalla data del 01.01.2024 sino al 31.12.2027.

In casi eccezionali, il contratto in corso di esecuzione può essere prorogato per il tempo strettamente necessario alla conclusione della procedura di individuazione del nuovo contraente se si verificano le condizioni indicate all'articolo 120, comma 11, del Codice. In tal caso il contraente è tenuto all'esecuzione delle prestazioni oggetto del contratto agli stessi prezzi, patti e condizioni previsti nel contratto.

ART. 23 - STIPULA -SPESE CONTRATTUALI

L'ASP provvederà alla stipula del contratto tramite sottoscrizione digitale di scrittura privata elaborata dal Mercato elettronico.

Trova applicazione quanto previsto dall'art. 18 del d.lgs. 36/2023.

Sono a carico dell'affidatario tutte le spese del contratto e dei relativi oneri connessi alla sua stipulazione, compresi quelli tributari, fatta eccezione per l'imposta sul valore aggiunto che resta a carico della committente. Per l'imposta di bollo, si rinvia a quanto previsto dall'allegato I.4 del d.lgs. 36/2023 nonché agli atti dell'Agenzia delle Entrate:

- circolare 22/E/2023
- risoluzione 37/E/2023
- provvedimento direttoriale prot. n. 240013/2023
- interpello 446/2023.

ART. 24 - TRATTAMENTO DATI PERSONALI

Ai sensi del Regolamento UE 2016/679 si informa che ASP "REGGIO EMILIA – Città delle persone", con sede in via Pietro Marani 9/1 a Reggio Emilia, è il titolare dei dati personali e si impegna a rispettare il carattere riservato delle informazioni fornite dagli operatori economici. Tutti i dati forniti saranno trattati solo per le finalità connesse e strumentali al presente contratto, nel rispetto delle disposizioni normative vigenti. In relazione ai suddetti dati l'interessato può esercitare i diritti sanciti dall'art.13 del Reg. EU 679/2016.

Il Responsabile per la protezione dei dati per l'ASP "REGGIO EMILIA – Città delle persone", è la Società Lepida SPA con sede in Via della Liberazione 15 Bologna. Il trattamento dei dati raccolti viene effettuato con strumenti manuali, informatici o telematici,esclusivamente per fini istituzionali e precisamente in funzione e per i fini e tempi della presente procedura. L'informativa completa di cui all'art. 13 REG. UE n. 679/2016 è pubblicata sul sito istituzionale www.asp.re.it nella sezione " Informative Privacy".

Con la sottoscrizione del contratto l'Appaltatore autorizza al trattamento dei dati personali, limitatamente e ai fini della presente procedura.

ART. 25 – DOMICILIO DELL'AFFIDATARIO E REFERENTE/RESPONSABILE DEL CONTRATTO PER L'APPALTATORE

Agli effetti del contratto, l'affidatario elegge domicilio presso _____ in _____, via _____, obbligandosi di informare il RUP di ogni variazione. In difetto il suddetto domicilio si intende fin d'ora eletto presso la sede della committente. L'affidatario dichiara che _____ nato a _____ il _____ e domiciliato/residente a _____ via _____, in funzione di _____, rappresenterà l'impresa nell'esecuzione del contratto.

Allegati n. 2

- *Data Brench*
- *Privacy*

IL DIRIGENTE
AREA RISORSE UMANE E FINANZIARIE
Dott. Teodoro Vetrugno

Teodoro
Vetrugno
30.11.2023
16:28:27
GMT+01:00

Allegato 1)

Accordo per il 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 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.

Phishing	Truffa effettuata su Internet, che sfrutta tecniche di ingegneria sociale, attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso.
Furto/smarrimento totale o parziale di apparecchiature che contengono dati sensibili	Il furto o smarrimento di singoli dispositivi di memorizzazione (hard disk, memorie di massa rimovibili ecc) oppure dei computer/server che li ospitano. Una violazione dei dati personali sensibili contenuti configura una condizione di data breach che richiede, ai sensi del GDPR, l'attivazione delle specifiche procedure di notifica verso l'autorità Garante e gli utenti coinvolti
Multiplo	Incidente di sicurezza che comprende due o più di quelli sopra elencati.
Malfunzionamento grave	Danneggiamento di un componente hardware o software, oppure degrado delle performance per cause esterne che possa arrecare impatti gravi alla disponibilità di servizio.
Disastro	Qualsiasi evento distruttivo, non provocato direttamente da azione di operatori informatici (es.: black out, incendio, allagamento, terremoto) in grado di condizionare direttamente l'operatività dei sistemi informatici.

Il **Referente**, a seguito della verifica della sussistenza di un reale incidente, effettua una **prima valutazione sull'impatto dell'incidente** ai fini di indirizzare in modo efficace le risorse necessarie alla sua gestione. Tale attività consiste in una prima classificazione della sua portata in base ai seguenti parametri:

- il livello di criticità della risorsa ICT coinvolta, determinato in base alle valutazioni inerenti la Business Impact Analysis. (in caso di coinvolgimento di più risorse verrà assunto come tale quello a maggiore criticità)
- il numero di risorse informatiche coinvolte, inteso come numero di server/applicazioni;
- il numero di utenti o postazioni di lavoro potenzialmente impattati dalla indisponibilità del servizio informatico;
- l'eventuale coinvolgimento di risorse ICT/utenti esterni all'organizzazione;
- l'esposizione su Internet del servizio;
- il tipo di danno arrecato (economico, immagine, mancato adempimento normativo ecc.);
- gli enti o le organizzazioni coinvolte nell'incidente;
- l'eventualità di coinvolgere le forze dell'ordine a causa di possibili risvolti di natura penale.

– In questa fase il Referente della sicurezza informatica del gruppo sicurezza ICT, anche coinvolgendo il referente della società incaricata della progettazione e della tenuta del sistema informatico aziendale e i tecnici informatici a disposizione dell'Azienda, deve anche stabilire la **gravità** dell'incidente di sicurezza. Per fare ciò può inizialmente avvalersi della seguente matrice contraddistinta da una valutazione di tipo qualitativo, ma la classificazione della gravità dell'incidente è comunque a sua totale discrezione.

Gravità incidente di sicurezza	***Descrizione***

Alta	Il grado di compromissione di servizi e/o sistemi è elevato. Si rilevano danni consistenti sugli asset. Il ripristino è di medio o lungo periodo. L'incidente presenta una tra le seguenti condizioni: • Danni a persone e rilevanti perdite di produttività • Compromissione di sistemi o di reti in grado di permettere accessi incontrollati a informazioni confidenziali • Siti web violati o utilizzati a fini di propagazione di materiale terroristico o pornografico • Frode o attività criminale che coinvolga servizi forniti dall'ente • Impossibilità tecnica di fornire uno o più servizi critici a un elevato numero di utenti per un intervallo di tempo superiore ai 30 minuti nell'arco di una giornata • Impossibilità tecnica di fornire uno o più servizi di criticità media per un periodo di tempo superiore ai 2 giorni lavorativi • Significativa perdita economica, di immagine e/o reputazione nei confronti del pubblico o degli utenti
Media	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta". Il grado di compromissione di servizi e/o sistemi è di una certa rilevanza e possono essere rilevati danni sugli asset di una certa consistenza. Il ripristino ha tempi che non compromettono la continuità del servizio L'incidente presenta una tra le seguenti condizioni: • Compromissione di server • Degrado di prestazioni relativo ai servizi offerti dall'ente con conseguente perdita di produttività da parte degli utilizzatori • Attacchi che provocano il funzionamento parziale o intermittente della rete • Impossibilità tecnica di fornire uno o più servizi critici ad un elevato numero di utenti per intervalli di tempo inferiori ai 30 minuti di tempo ripetuti su più giornate • Impossibilità tecnica di fornire uno o più servizi critici ad una piccola parte di utenti per un periodo di tempo superiore ai 30 minuti di tempo nell'arco di una o più minuti ei tempo nell'arco di una o più giornate • Basso impatto in termini di perdita economica, di immagine e/o reputazione nei confronti degli utenti
Bassa	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta o media". Non vengono compromessi asset o servizi. L'incidente presenta le seguenti condizioni: • Interruzione dell'attività lavorativa di un numero ristretto di dipendenti e per un breve periodo di tempo. • Contaminazioni da virus in un medesimo sito ma comunque identificate dai sistemi anti-malware • Nessuna o limitata perdita di operatività o di business da parte di un ridotto numero di dipendenti.

Poiché per alcuni incidenti può risultare difficile assegnare un livello di gravità definitivo prima che l'analisi sia completa, occorre che la valutazione sia effettuata sulla base delle evidenze note sino a quel momento, assumendo che la gravità potrebbe molto probabilmente aumentare nel caso in cui non si effettui alcuna operazione di contenimento.
Il Referente, verificare comunque ciclicamente, nel periodo in cui l'incidente è in corso, la gravità assegnata allo stesso, in quanto essa può variare nel tempo.

Effettuata una prima analisi, ancorché non definitivamente conclusa, il Referente informa tempestivamente il **Responsabile per la gestione della sicurezza ICT,** che provvede ad attivare il **Gruppo per la Gestione della Sicurezza,** deputato alla gestione incidenti e, in caso di *data breach,* informa immediatamente il DPO, e il Legale Rappresentante dell'Azienda. Nel contempo, il **Referente,** sulla base della gravità appurata dell'incidente, **attiva direttamente** la **procedura di gestione incidenti,** secondo quanto più dettagliatamente descritto al successivo punto D).

B. VALUTAZIONE DEI RISCHI DERIVANTI DAL VERIFICARSI DEL DATA BREACH

In caso di *data breach* il Gruppo per la gestione della Sicurezza ICT valuta i rischi per i diritti e le libertà delle persone fisiche, utilizzando i criteri di seguito indicati:

- la tipologia di violazione, ovverosia il tipo di violazione così come declinata nel precedente paragrafo 3;
- la natura dei dati violati, valutando che più i dati sono "sensibili" e maggiore è il rischio di danni per le persone fisiche;
- il volume dei dati violati, considerando che la violazione di diverse tipologie di dati comporta un rischio maggiore rispetto alla violazione di una sola tipologia;
- il numero di individui cui si riferiscono i dati violati, considerando che, generalmente, maggiore è il numero di individui interessati, maggiore è l'impatto di una violazione. Tuttavia, una violazione può avere un impatto grave anche su un solo individuo, a seconda della natura dei dati personali e del contesto in cui è stato compromesso;
- caratteristiche speciali degli individui cui si riferiscono i dati violati, ad esempio minorenni o persone vulnerabili;
- il grado di identificabilità delle persone, considerato che l'identificazione potrebbe essere possibile direttamente dai dati personali violati senza alcuna ricerca speciale necessaria per scoprire l'identità dell'individuo, oppure potrebbe essere estremamente difficile abbinare i dati personali a un particolare individuo, ma potrebbe comunque essere possibile a determinate condizioni (sono, quindi, considerati tutti i mezzi di cui ci si possa avvalere per identificare le persone fisiche);
- la gravità delle conseguenze per gli individui: tale criterio è strettamente connesso alla tipologia di dati violati. Deve essere considerato che una violazione di riservatezza può occorrere anche nel caso in cui dei dati personali siano comunicati a un terzo, pur non autorizzato, ma conosciuto e "fidato". In tali casi, evidentemente la valutazione di tale criterio abbasserà il livello di gravità delle conseguenze per gli individui. Nel caso in cui i dati personali siano nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose, il livello di rischio potenziale sarà più elevato.

In caso di *data breach* il Data Protection Officer (DPO) è sempre coinvolto nella valutazione dei rischi per i diritti e le libertà delle persone fisiche ed esprime anche formale parere sulla necessità di effettuare la notifica.

C. COMUNICAZIONE DEGLI INCIDENTI

La notifica della violazione al Garante

Nei casi in cui l'incidente consista in una violazione di dati personali, il Titolare , nella persona del Legale Rappresentante pro tempore, deve notificare l'incidente al Garante per la protezione dei dati personali se, sulla scorta della valutazione approfondita, strutturata e documentata di cui al paragrafo precedente, si assuma come probabile che la violazione dei dati personali presenti effettivamente un rischio per i diritti e le libertà delle persone fisiche.

La comunicazione al Garante, da redigere sulla base del modello allegato al presente documento quale parte integrante e sostanziale (all.1), , deve ricomprendere ogni informazione utile, oltre che la descrizione:

- della natura della violazione dei dati personali;
- delle categorie e del numero approssimativo di interessati in questione, nonché delle categorie e del numero approssimativo di registrazioni dei dati personali in questione;
- delle probabili conseguenze della violazione dei dati personali;
- delle misure adottate, o di cui si propone l'adozione, per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
- i recapiti del Data Protection Officer.

La notifica della violazione agli interessati.

Alcune violazioni di dati, quelle che comportano un rischio elevato per i diritti e le libertà delle persone fisiche devono essere comunicate agli interessati senza ingiustificato ritardo. Tale comunicazione, da redigere in aderenza all'allegato 1 del presente documento ,deve essere formulata con linguaggio chiaro e comprensibile agli utenti e deve ricomprendere:

- la descrizione della natura della violazione;
- i recapiti del Data Protection Officer;
- la descrizione delle probabili conseguenze della violazione;
- le misure adottate, o di cui si propone l'adozione, per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Nel caso in cui il numero di interessati lo consenta, la comunicazione deve essere inviata a mezzo mail (o pec, o sms) e comunque con avviso pubblicato sul sito istituzionale. Nel caso in cui il numero di soggetti coinvolti sia particolarmente ingente, è sufficiente effettuare la comunicazione dell'avvenuta violazione di dati utilizzando il sito istituzionale.

D. ATTIVAZIONE DELLA PROCEDURA E MONITORAGGIO DELLE ATTIVITÀ

L'attivazione della procedura di gestione incidenti, è a carico del **Referente per la gestione della sicurezza informatica**, il quale, a seconda della gravità attribuita in fase di identificazione dell'incidente, utilizzerà diverse modalità di attivazione e tracking.

<u>Incidente di gravità "Alta"</u>

Il Referente per la gestione della sicurezza informatica informa immediatamente il **Responsabile della Sicurezza** per il coinvolgimento del gruppo Gestione Sicurezza mediante l'invio dell'apposito Rapporto incidente di sicurezza, compilando soltanto le parti che in questa fase è possibile conoscere.

Lo scopo principale di questa prima fase è di attivare il gruppo sicurezza per la gestione dell'incidente ed eventualmente anche informare il DPO nel caso di un *data breach*. Il Rapporto incidente di sicurezza sarà poi completato in tutte le sue parti in fase di chiusura dell'incidente.

Il **Responsabile della Sicurezza,** deve conservare per la durata di cinque anni il Rapporto, in formato elettronico, in una cartella soggetta a backup periodico e ad accesso opportunamente limitato.
E' altresì fondamentale che tutte le operazioni eseguite per la gestione di un eventuale incidente siano opportunamente tracciate (es. strumento informatico di ticketing o altro), permettendo in tal modo di poter identificare tutte le risorse coinvolte nelle operazioni tecniche di gestione e poterle eventualmente indicare in ambito giudiziale come testimoni.
Le indagini svolte e le operazioni di gestione formano quindi una base dati che andrà ad incrementare la conoscenza dell'Azienda in merito agli incidenti di sicurezza informatica.
Nel caso in cui l'incidente di sicurezza abbia un impatto sulla continuità operativa per un tempo di disservizio inaccettabile per gli utenti interni ed esterni (superiore al RTO dichiarato in sede di BIA), è necessario attivare il Gruppo sicurezza

Incidente di gravità "Media" o "Bassa"
In caso di incidente di gravità media o bassa, l'incidente può essere completamente gestito dal referente per la gestione della sicurezza informatica fermo restando il coinvolgimento del Responsabile della Sicurezza e, nel caso di un *data breach*, del DPO. In tale caso non è necessaria (anche se è consigliabile) la stesura del Rapporto di Incidente di Sicurezza, ma è comunque necessario tracciare opportunamente le operazioni permettendo in tal modo di poter identificare tutte le risorse coinvolte nelle operazioni tecniche di gestione e di poterle eventualmente indicare in ambito giudiziale come testimoni.
Anche in questo caso le indagini svolte e le operazioni di gestione formano una base dati che andrà a incrementare la conoscenza dell'Azienda in merito agli incidenti di sicurezza informatica.
I dati raccolti saranno resi disponibili, attraverso diversi profili di consultazione, anche a fini statistici, al Responsabile della Sicurezza, ai membri del gruppo sicurezza e al Legale Rappresentante dell'Azienda.

6.2 Contenimento, rimozione e ripristino

Le operazioni di contenimento hanno due importati fini:
- evitare che il danno si propaghi, o almeno limitarne la diffusione;
- acquisire le eventuali evidenze digitali di reato prima che queste possano essere compromesse.

A tal fine è necessario:
- identificare tutti i sistemi che possono essere stati compromessi o sui cui sia possibile raccogliere eventuali evidenze digitali di reato;
- effettuare delle copie delle eventuali evidenze digitali di reato in modo valido dal punto di vista forense;
- documentare in modo dettagliato tutte le operazioni eseguite, onde evitare, in un eventuale ambito giudiziale, possibili contestazioni sulla correttezza delle operazioni eseguite;

Le attività di contenimento dovranno essere eseguite da personale qualificato, ovvero da sistemisti o esperti applicativi appositamente addestrati per eseguire le operazioni necessarie, dipendenti dell'Azienda o dalla medesima incaricati.

Tutte le operazioni eseguite saranno comunque sotto la responsabilità del Referente per la sicurezza informatica il quale dovrà riportare nel Rapporto di incidente:
- data e ora delle azioni eseguite sui sistemi, applicazioni o dati;
- generalità delle risorse che hanno materialmente eseguito le operazioni;
- risultati conseguiti.

Il Referente per la sicurezza informatica dovrà comunicare al Responsabile della sicurezza quanto eseguito al termine di questa fase, raccordandosi poi con il Responsabile del Servizio Affari

Generali e Giuridico Legali per la trasmissione di copia della documentazione utile ai fini della proposizione delle azioni legali di competenza.
Le operazioni di contenimento possono essere di due tipologie: a breve termine e a lungo termine.

A. CONTENIMENTO A BREVE TERMINE

Le operazioni di contenimento a breve termine mirano a mettere in sicurezza gli eventuali sistemi interessati da un incidente, senza alterarne la configurazione o inquinare eventuali evidenze digitali di reato.
Come esempi, non esaustivi, di azioni di contenimento a breve termine si possono indicare:

- creazione di regole firewall atte a bloccare l'accesso ai sistemi coinvolti;
- disabilitazione di account utente sui sistemi centralizzati di autenticazione;
- cambio di configurazione sui sistemi DNS;
- disconnessione dei sistemi coinvolti dalla rete mediante riconfigurazione di apparati di rete.

Dopo aver messo in sicurezza i sistemi coinvolti nell'incidente, mediante l'operazione di contenimento a breve termine, è possibile procedere all'acquisizione di eventuali evidenze digitali (es. mediante copia forense dei dischi) oppure procedere con l'esecuzione di normali backup atti a mettere in sicurezza i dati per poterli riutilizzare nella eventuale ricostruzione del sistema colpito dall'incidente.
E' necessario procedere all'acquisizione forense delle evidenze digitali di reato in ogni caso in cui si preveda un prosieguo in ambito legale come per esempio:

- accessi abusivi a sistemi o informazioni;
- attività illecite commesse da dipendenti o da utenti dei servizi aziendali comunque mediante il sistema informativo gestito dell'Azienda;
- interruzione di pubblici servizi critici;
- violazioni della privacy di dipendenti, utenti e cittadini;
- utilizzo illegale dei sistemi per perpetrare truffe o diffondere materiale illecito.

Quando invece l'incidente è causato da malfunzionamenti o errori umani è possibile procedere eseguendo una normale operazione di backup relativa a dati o configurazioni eventualmente presenti sul dispositivo coinvolto nell'incidente. Questa operazione potrà quindi essere eseguita utilizzando i sistemi e i programmi utilizzati per effettuare le comuni operazioni di backup e hanno lo scopo di mettere in sicurezza le informazioni necessarie per un' eventuale reinstallazione del dispositivo.

B. CONTENIMENTO A LUNGO TERMINE

Il contenimento a lungo termine comporta l'esecuzione di operazioni tecniche direttamente sui sistemi coinvolti nell'incidente; per questo motivo questa azione deve essere eseguita solo dopo aver messo in sicurezza le evidenze digitali di reato o i dati presenti sul sistema impattato.
Tali operazioni mirano a rendere i sistemi coinvolti più sicuri e permettono di lasciarli in attività sino al momento in cui sia possibile procedere a operazioni più complesse di rimozione delle cause.
A titolo esemplificativo e non esaustivo, si possono indicare quali operazioni di contenimento a lungo termine:

- installazione di patch o aggiornamenti di sistema e/o applicativi;
- cancellazione di file o dati;
- arresto di servizi o processi malevoli;
- cambio di configurazione di programmi.

Al termine di queste operazioni i sistemi coinvolti nell'incidente non possono ancora dichiararsi sicuri, ma è possibile utilizzarli temporaneamente sino a quando non sia possibile procedere con le operazioni di rimozione definitiva di quanto ha scatenato l'incidente.
Durante questa fase, possono emergere diverse necessità, come per esempio:

- allocare risorse economiche per la fase di acquisizione forense/backup e le successive fasi di gestione;
- isolare e/o arrestare eventuali servizi o sistemi critici di produzione coinvolti;
- valutare eventuali conseguenze legali;
- relazionarsi con le Aree/Servizi dell'Azienda per comunicare eventuali disservizi.

In tali casi il Referente per la sicurezza informatica può operare le corrette scelte in autonomia, comunicando al Responsabile della Sicurezza le eventuali azioni che saranno intraprese e raccordandosi, secondo quanto precedentemente indicato, con il Responsabile del Servizio Affari Generali e Giuridico Legali.

C. RIMOZIONE

Le operazioni di rimozione sono volte all'eliminazione definitiva del problema o della vulnerabilità utilizzata per compromettere un sistema coinvolto in un incidente e riportarlo a un livello di sicurezza elevato.
Le attività che sono solitamente eseguite in questa fase possono essere di diverso tipo, per esempio:

- aggiornamento di release dei sistemi operativi o del software presente (per rimuovere eventuali vulnerabilità di sicurezza);
- rimozione di eventuali servizi o software che, utilizzati in modo malevolo, possono compromettere il sistema stesso (hardening);
- in alcuni casi, come, ad esempio, per le infezioni da virus/malware, può essere più semplice e meno oneroso economicamente, ricostruire l'intera macchina reinstallando il software a partire dal sistema operativo.

La valutazione dell'impatto tecnico ed economico delle operazioni di rimozione deve essere eseguita dal Gruppo gestione sicurezza, eventualmente coinvolgendo tutti i soggetti interessati e fornendo al Responsabile della sicurezza, tramite un report di dettaglio, le indicazioni degli eventuali costi da sostenere e dei tempi necessari al ripristino, affinché il medesimo possa informare il Legale rappresentante e il Consiglio di Amministrazione.

Poiché l'operazione di contenimento a lungo termine non è da considerarsi risolutiva del problema, ma solo ed esclusivamente un'azione a titolo temporaneo, l' Azienda si impegna a contenere i tempi necessari per poter procedere alla fase di rimozione ai tempi tecnici strettamente necessari alla definizione dell'intervento, al reperimento delle relative risorse economiche e alle operazioni di approvvigionamento.

D. RIPRISTINO

In questa fase le operazioni eseguite mirano principalmente a verificare che i sistemi coinvolti nell'incidente siano stati correttamente riattivati e che siano nuovamente sicuri, per considerare l'incidente effettivamente chiuso.
E' necessario ottenere un elevato grado di certezza che quanto accaduto non possa ripetersi; per questo motivo si rende necessario definire con il dovuto dettaglio tutte le fasi di riattivazione di un sistema coinvolto, sia nei modi che nei tempi attesi per il ripristino, sia nei controlli da effettuare per certificare il ritorno alla normalità.

6.3 Attività post-incidente

La decisione del momento in cui un sistema coinvolto in un incidente possa ritornare in produzione è in carico al Referente per la sicurezza informatica che, in collaborazione con il Gruppo per la gestione della sicurezza ed eventuali gruppi di supporto tecnici coinvolti, definisce un piano di riattivazione dei diversi servizi impattati dall'incidente.

In alcuni casi specifici, può essere necessario riattivare i sistemi in un periodo non lavorativo (es. nelle ore notturne oppure nei fine settimana) per dare la possibilità alle strutture che hanno in carico la gestione dei sistemi stessi di operare senza che siano presenti richieste di accesso da parte di utenti che non siano quelli deputati all'esecuzione di eventuali test di funzionamento.

Onde verificare che le operazioni di ripristino siano avvenute correttamente, si rende necessario monitorare il corretto funzionamento dei sistemi per un periodo di tempo adeguato, per cui potrebbe esservi la necessità di attivare ulteriori controlli utilizzando gli strumenti di monitoraggio in uso, oppure aumentando il livello di profondità degli eventi da registrare nei file di log applicativi o dei sistemi operativi.

Sarà il Referente per la sicurezza informatica a richiedere la modifica o l'implementazione di nuove regole di monitoraggio ai soggetti preposti.

Tutti gli incidenti di sicurezza devono essere documentati. Tale documentazione, unitamente alle evidenze degli incidenti, devono essere debitamente archiviate.

Sono documentati e archiviati, in modalità distinguibile rispetto ai restanti incidenti di sicurezza, tutti i data *breach,* seppure non notificati all'Autorità Garante e/o agli interessati.

Dal punto di vista tecnico le operazioni di chiusura dell'incidente, consistono nella dichiarazione della fine dello stato di incidente e nella compilazione del report relativo all'incidente stesso da parte del Referente per la sicurezza informatica.

Il report, firmato digitalmente dal Responsabile della Sicurezza, tramite procedura di hashing, a garanzia della sua integrità, dovrà essere consegnato al Gruppo sicurezza e dovrà essere inviato in forma riservata sotto forma di relazione sull'esito dell'incidente di sicurezza al Legale Rappresentante, al Consiglio di Amministrazione e ai Dirigenti responsabili dei Servizi coinvolti.

Il Responsabile della Sicurezza deve conservare il Rapporto in un repository ad accesso limitato ai membri del proprio staff, per cinque anni o per tutto il tempo ritenuto necessario (ad esempio allo svolgimento di indagini, nel caso di conseguenze penali, o perlomeno alla definitiva rimozione delle cause scatenanti l'incidente).

In seguito alla chiusura dell'incidente, dovranno essere valutate tutte le operazioni eseguite per la gestione dello stesso, evidenziando sia i punti in cui queste sono state eseguite in armonia con le procedure e le aspettative, sia eventuali problemi sorti durante lo svolgimento delle operazioni.

Le informazioni raccolte durante la gestione dell'incidente dovranno essere archiviate, in forma anonimizzata nella knowledge base dell' Azienda (consultabile ad accesso ristretto in base al ruolo ricoperto nel processo di gestione incidenti).

I punti critici rilevati durante l'esecuzione delle operazioni saranno condivisi con i componenti del team di gestione degli incidenti e si provvederà nel più breve tempo possibile a predisporre quanto necessario per eliminarli o mitigarli, migliorando quindi sia la procedura tecnica di gestione, sia la capacità di operare della struttura preposta, sia le infrastrutture e i sistemi.

Per la rilevazione di eventuali criticità il Gruppo di gestione della sicurezza, eventualmente allargato a figure che siano state parte attiva nella gestione dell'incidente, verificherà tramite apposita checklist se:

- la procedura di gestione incidenti sia stata correttamente eseguita;
- la procedura sia risultata adeguata al contesto;
- si siano presentati aspetti che abbiano rallentato la risoluzione dell'incidente;
- si siano presentati elementi che si ritiene debbano essere cambiati in modo da rendere il processo di gestione degli incidenti più efficace ed efficiente;
- sia necessario aggiornare il metodo di analisi della gravità a valle dell'incidente;

- siano necessarie delle azioni correttive da intraprendere in fase di mitigazione dei rischi onde evitare che l'incidente possa riaccadere;
- sia necessario modificare le policy aziendali dal punto di vista tecnico (es.: aggiungere file con una determinata estensione tra quelli bloccati dal sistema antivirus;
- sia necessario aggiornare e/o migliorare gli interventi formativi al fine di istruire il personale aziendale sulle problematiche inerenti la sicurezza e la privacy dei dati;
- siano necessarie risorse addizionali (es.: personale, tools, strumenti hardware o software) per rendere il processo di gestione degli incidenti più efficace ed efficiente;
- siano necessarie modifiche e/o riconfigurazioni del software (es.: aumentare frequenza di aggiornamento delle firme dei software antivirus e/o anti-intrusione e, modificare il livello di dettaglio fornito dai sistemi di difesa perimetrali);

Scopo di tale operazione è quello di verificare che il processo di gestione incidenti sia risultato adeguato a fronteggiare la situazione e far si che le considerazioni che ne scaturiscono diventino patrimonio comune all'interno del team di gestione degli incidenti.

Per questo motivo, entro breve termine dalla chiusura formale di un incidente, il Responsabile della Sicurezza convoca il Gruppo per la gestione della sicurezza e le eventuali figure che sono state parte attiva nella gestione dell'incidente, con l'obiettivo di valutare collegialmente l'efficacia della procedura di gestione degli incidenti e definire in un apposito verbale le considerazioni e le operazioni che possano portare a migliorare l'intera procedura.

Allegato 1 : Rapporto incidente di sicurezza

1. Premessa:

(breve descrizione dell'incidente, dei sistemi coinvolti, degli utenti su cui l'incidente ha impatto, della durata dell'incidente, delle modalità attraverso le quali si è venuti a conoscenza dell'incidente)

2. Descrizione dettagliata dell'incidente:

(causa che ha determinato l'incidente);
(sistemi coinvolti);
(eventuali disservizi causati);
(utenti coinvolti);
(eventuali enti esterni coinvolti);
(dettagli tecnici rilevanti: es. log dei sistemi, traffico di rete, schermate, e- mail, ecc.).

3. Rilevazione dell'incidente:

(modalità attraverso le quali si è venuti a conoscenza dell'incidente:

- *notifica automatica tramite sistemi di rilevazione*
- *individuazione a seguito di verifiche di sicurezza*
- *segnalazione da parte di un utente*
- *altro).*

4. Contromisure adottate

(descrizione delle azioni intraprese per contenere i danni causati dall'incidente e per ripristinare i sistemi)

5. Conclusioni

(impatto dell'incidente sui sistemi o sui servizi);
(elementi che avrebbero consentito di prevenire il verificarsi dell'incidente);
(ulteriori azioni di approfondimento necessarie).

6. Note
(eventuali considerazioni sull'incidente, suggerimenti, adeguamenti da effettuare, ecc.).

7. Riferimenti
(eventuali riferimenti ad allegati o altri documenti).

….. , li ……. Responsabile della Sicurezza
(nome e cognome)