Mod A_2022

1 Livelli di servizio

Tempi di attivazione: entro 1 settimana dall'ordine si attiva il processo di censimento e configurazione dei servizi. La pianificazione del progetto è poi concordata con l'Ente.

Tempi di disattivazione: entro 1 settimana dalla richiesta o dalla scadenza del contratto. Con modalità riportate nel paragrafo "Privacy, trattamento dei dati personali e riservatezza".

Il servizio verrà erogato in modalità Cloud. L'erogazione avverrà su data center Microsoft Azure dove vengono esposti i servizi web e i portali ad uso del cittadino e dell'Ente.

L'archivio dei pagamenti in attesa e tutti i connettori verso il Nodo dei Pagamenti e SPC vengono ospitate su Data Center di SIA SpA.

La piattaforma Plug&Pay offerta è disponibile 365x24x7.
Disponibilità e Disaster Recovery (DR) del Data Center:
Modalità On line: Disponibilità 98%, DR: RTO: 24h, RPO:2 min
Modalità Massiva batch: Disponibilità 95%, DR: RTO: 48h, RPO:3 ore
RTO (Recovery Time Objective) corrispondete all'intervallo di tempo compreso tra la dichiarazione dello stato di crisi ed il momento in cui il servizio è nuovamente disponibile al suo livello minimo.
RPO (Recovery Point Objective) eventuali dati persi durante il disastro.

1.1 regole di mantenimento delle informazioni in conformità con la direttiva GDPR

A seguito dell'implementazione delle politiche di trattamento dati in conformità con la direttiva GDPR, vengono applicate le seguenti regole di mantenimento delle informazioni gestite dal servizio Plug&Pay in modo da ottemperare al principio di trattamento minimo necessario all'esecuzione del servizio, previsto dalla normativa GDPR e al contempo garantire la conformità con le regole di tracciamento dei pagamenti.
Le regole applicate per la procedura di svecchiamento, secondo il principio di trattamento minimo necessario all'esecuzione del servizio, riguardano:

- POSIZIONI PAGATE: eliminate dopo 24 mesi dalla data di pagamento.
  POSIZIONI NON PAGATE: eliminate dopo 24 mesi dalla data di scadenza o 5 anni dalla pubblicazione. Le posizioni caricate senza la data di scadenza verranno eliminate dopo 24 mesi dalla data di caricamento. Ad eccezione delle posizioni generate da richieste di pagamento spontaneo mantenute solo 12 mesi rispetto la data di carico sui sistemi.
- POSIZIONI REVOCATE (cancellazioni logiche a seguito di operazioni di eliminazione): eliminate e dopo 30 giorni dalla data di revoca/eliminazione.
- DATI ASSOCIATI ALLE FORNITURE MASSIVE DI POSIZIONI: eliminate dopo 24 mesi dalla data di caricamento della fornitura.

Il servizio prevede comunque la possibilità opzionale di un prolungamento del mantenimento dei dati.

- Il prolungamento potrà essere effettuato per una durata multipla di anno (1 anno, 2 anni ecc.).
- Si potrà limitare il prolungamento ai soli servizi di pagamento per i quali la misura è necessaria e giustificata.
- Il prolungamento sarà a titolo oneroso e comporterà un modesto aumento del canone base in ragione della durata e del numero di servizi con mantenimento prolungato.

In ogni caso trascorsi i 24 mesi le posizioni debitorie non pagate saranno disponibili per uso amministrativo ma non per il pagamento. Pertanto sarà inibita l'eventuale stampa del relativo avviso di pagamento, il pagamento tramite PosPA e comunicazioni tramite app IO.

2 Help Desk e Incident Management

HELP DESK

L'Help Desk è a disposizione per **supporto riguardante l'operatività ordinaria** quali ad esempio configurazione servizi, recupero ricevute telematiche, recupero rendicontazioni, caricamento/pubblicazioni forniture, inserimento puntuale, ricerca posizioni/pagamenti, utilizzo del portale di back office.
Il servizio è disponibile **dal lunedì al venerdì, dalle 09.00 alle 13.00 e dalle 14.30 alle 17.00**.

SERVICE DESK

Il Service Desk è a disposizione per la segnalazione di anomalie e malfunzionamenti che causano la riduzione o l'interruzione sistematica del servizio, quali ad esempio non corretto funzionamento del portale di backoffice, irregolare funzionamento del processo di pagamento.
Il servizio di assistenza telefonica al numero **340.1145693** è attivo **dal lunedì al venerdì, dalle 09.00 alle 13.30 e dalle 14.30 alle 18.00 ed il sabato dalle 09.00 alle 14.00**.

Per ricevere assistenza occorre inviare una segnalazione all'indirizzo e-mail **servicedesk.plugandpay@e-fil.eu**.

Per permettere una rapida risoluzione della problematica che hai riscontrato, riporta tutti i dati in tuo possesso utili per l'individuazione del caso.

- Denominazione dell'Ente
- Portale su cui si è verificata la problematica (Pagamento o Backoffice)
- Descrizione della problematica
- Numero di telefono per eventuali comunicazioni (facoltativo)

Il service desk a fronte dell'analisi della segnalazione verificherà la gravità ed assegnerà la priorità per la risoluzione.

Incidente (in assenza di dichiarazione di disastro) che causa **l'interruzione** o la **riduzione significativa** delle prestazioni del servizio:

- Portale di BackOffice
- Portale di pagamento
- Web Service

Risoluzione entro 4 ore lavorative

Incidente (in assenza di dichiarazione di disastro) che causa una **parziale** riduzione delle funzionalità:

- Portale di BackOffice
- Portale di pagamento
- Web Service

Risoluzione entro 1 gg lavorativo.

Incidente (in assenza di dichiarazione di disastro) che non causa una significativa riduzione delle funzionalità (non bloccante perché esiste una funzionalità alternativa) o impatta su una funzionalità marginale.

Risoluzione entro 2 gg lavorativi.

Le tempistiche lavorative si riferiscono a Lun-Ven 9-18, Sabato 9-13 esclusi i festivi (1 gennaio, 6 gennaio, lunedì di Pasqua, 25 aprile, 1 maggio, 2 giugno, 15 agosto, 1 novembre, 8 dicembre, 25 e 26 dicembre).

3 Policy per la gestione della Sicurezza delle Informazioni e Privacy

Crittografia Nell'ambito della sicurezza informatica la crittografia rappresenta uno strumento fondamentale che viene utilizzato non solamente per proteggere i dati, archiviati o in transito, da accessi non autorizzati, ma anche e soprattutto da divulgazioni accidentali che potrebbero avvenire per imperizia degli utenti che trattano le informazioni, furto, smarrimento dei device o altro evento infausto.

A tal fine si adottano procedure si sicurezza per la protezione di dati, dischi, virtual machine e così via..
Parliamo di:

- Crittografia dei Dati/Dischi fissi e rimovibili
- Crittografia dei file di configurazione delle applicazioni
- Crittografia delle comunicazioni (sFTP, https)

Gestione dei Cambiamenti Efil persegue l'evoluzione dei sistemi e dei servizi erogati per garantire funzionalità rispondenti alle esigenze dei clienti, le migliori metodologie e tecniche per la sicurezza delle informazioni nell'ambito della normativa e migliori pratiche.
Ogni cambiamento è sottoposto ad un rigoroso processo di progettazione, sviluppo, collaudo e messa in esercizio.
Ogni passo segue quindi procedure che hanno l'obiettivo di garantire che la catena fornisca al cliente un prodotto migliore ma nel contempo metta l'utente nelle condizioni di conoscere le nuove funzionalità e di utilizzarle al meglio.
Il cambiamento non deve causare disservizi, perdite di dati.
Il cambiamento deve essere accompagnato da documentazione e formazione all'utente.
Ove il cambiamento impatti sulle applicazioni del cliente verranno forniti con congruo anticipo tutti gli elementi tecnici per consentire l'adeguamento applicativo.
Gestione della Capacità Elaborativa E-Fil monitora costantemente la capacità elaborativa e di storage anche in cloud, per garantire sempre che le risorse siano adeguate ai livelli di servizio dichiarati. Raccoglie eventuali segnalazioni da parte degli utenti per rilevare situazioni di criticità e mette in atto adeguate azioni, di cambiamento applicativo, infrastrutturale o organizzativo per ripristinare i livelli di servizio dichiarati.
Le risorse cloud sono costantemente monitorate, CPU, Ram, Spazio disco delle VM. Numero di connessioni web instaurate correttamente, connessioni web con errore dei web server sono oggetto di monitoraggio ed analisi per garantire adeguata capacità elaborativa e evidenziare eventuali situazioni di cattivo utilizzo o attacco informatico.
Backup dei dati Efil, identifica nella protezione dei dati e nella disponibilità degli stessi uno dei valori principali da garantire e perseguire.
Per tale ragione l'azienda monitora tutte le fasi elaborative e di archiviazione, con l'obiettivo di assicurare la massima efficienza dei sistemi e la disponibilità degli stessi secondo gli SLA di servizio offerti. L'azienda monitora l'intera filiera elaborativa anche ove vengano utilizzati servizi di fornitori, quando questi impattano direttamente o indirettamente sulla protezione dei dati e sulla loro disponibilità.
Il backup dei dati, rappresenta la sicurezza che il dato può essere protetto e reso disponibile, integro per le funzionalità erogate. Una adatta politica di backup garantisce di minimizzare o eliminare eventuali perdite di dati a seguito di incidenti o malfunzionamenti dei sistemi di elaborazione.
L'azienda ha identificato i sistemi "Mission Critical" che hanno le esigenze più elevate di protezione e di disponibilità e per questi attiva azioni specifiche.
Il personale di monitoraggio e addetto all'erogazione viene formato ed istruito per la gestione di situazioni critiche attraverso l'applicazione di procedure di simulazione di situazioni di ripristino in emergenza.
Sviluppo sicuro del software. La progettazione e lo sviluppo di software sicuro rappresenta la base per la sicurezza delle informazioni gestite tramite applicazioni, siano esse ad uso dei clienti che delle procedure di elaborazione lato server.
Efil ha identificato alcune linee guida che costituiscono un insieme di best practices da seguire, al fine prevenire eventuali problematiche di sicurezza nel codice, e forniscono nel contempo uno strumento utile nell'individuazione di possibili vulnerabilità presenti nel codice sorgente e le relative contromisure da applicare.
L'obiettivo è quello di garantire che la sicurezza delle informazioni sia progettata e realizzata all'interno del ciclo di sviluppo dei sistemi informativi. Il software rappresenta un asset aziendale primario, in quanto rappresenta uno dei valori per cui l'azienda viene apprezzata sul mercato.

I punti salienti del ciclo del processo di sviluppo sono:

- Progettazione e Sviluppo del Software
- Controllo dei Cambiamenti di Sistema
- Test di Sicurezza e Strumenti di correttezza del codice
- Installazione e Protezione dei dati ambiente di collaudo
- Salvaguardia dell'asset aziendale

Sicurezza dell'infrastruttura di erogazione. Efil utilizza infrastrutture di erogazione ad alta disponibilità, che possono agevolmente gestire situazioni di disastro. L'infrastruttura cloud di riferimento è Microsoft Azure, che consente di scalare facilmente per adattarsi alle mutevoli esigenze elaborative, fornisce funzionalità di ridondanza geografica su siti Europei con tempi di copia dei dati pressoché nulli oltre che permettere una profilatura e logging degli accessi per tutti gli utenti compresi gli amministratori. Le immagini delle VM e i file di database sono criptati e quindi i dati inaccessibili.

Gestione della catena di fornitura ITC. Efil è attenta all'intera filiera di fornitura ITC, alla selezione e qualificazione dei fornitori che impattano sull'erogazione dei servizi ed in particolare sull'infrastruttura. Per questo motivo ha adottato soluzioni infrastrutturali di alto livello, Microsoft Azure per l'erogazione delle applicazioni web, web service e storage. Utilizzando quindi un approccio cloud moderno, sicuro e solido. La garanzia della continuità operativa passa quindi anche dai livelli di disponibilità e di disaster recovery che l'infrastruttura offre.

Per ambiti specialistici legati all'interfacciamento con il Nodo dei Pagamenti e SPC, invece utilizza servizi tecnologici di SIA S.p.a. leader nazionale per i servizi e le infrastrutture vocate al financing, garantendo quindi soprattutto alti livelli di sicurezza e disponibilità delle operazioni di interazione con gli attori del dominio (Nodo, PSP).

Con questi fornitori Efil ha attive relazioni contrattuali che garantiscono fornitura di servizi ITC adeguati agli SLA offerti, sia nella disponibilità, nel change management e dell'incident management.

E-FIL può avvalersi di società specializzate nella gestione dell'infrastruttura tecnologica, con contratti regolati dalle vigenti norme in ambito GDPR e in linea con le politiche aziendali per la sicurezza delle informazioni ai fini della compliance con il sistema di qualità ISO/IEC 27001 ed estensioni Cloud e Privacy.

Trasferimento delle informazioni. Efil, identifica nella protezione dei dati e nella disponibilità degli stessi uno dei valori principali da garantire e perseguire.

Per tale ragione l'azienda monitora tutte le fasi di trasferimento dati, con l'obiettivo di assicurare la massima sicurezza e riservatezza. L'azienda monitora l'intera filiera applicativa anche ove vengano utilizzati servizi di fornitori, quando questi impattano direttamente o indirettamente sulla protezione dei dati e sulla loro disponibilità.

L'azienda applica tutte le metodologie e tecnologie più evolute per garantire tali obiettivi.

Privacy, trattamento dei dati personali e riservatezza. Ai fini dell'esecuzione dei servizi abbinati alla presente licenza d'uso l'Ente, in qualità di Titolare del trattamento dei dati personali relativi ai dati di soggetti terzi, a valle della sottoscrizione del presente acquisto e prima che inizino i trattamenti dovrà nominare E-FIL s.r.l. quale Responsabile Esterno del trattamento dei dati ai sensi dell'articolo 28 del Regolamento 679/2016/UE (GDPR).

E-FIL si obbliga al puntuale rispetto delle norme e degli obblighi di riservatezza e sicurezza prescritti dal D. Lgs. 10/08/2018 n. 101 emesso in applicazione del già citato GDPR (Codice Privacy) e di tutte le eventuali successive disposizioni a carattere generale emanate dal Garante per la Protezione dei Dati Personali. I dati saranno utilizzati per le sole finalità di svolgimento delle prestazioni oggetto del presente Atto e per il tempo strettamente necessario all'espletamento delle stesse.

E-FIL è tenuta ad utilizzare i dati personali di cui verrà a conoscenza nel corso dell'esecuzione del presente Atto per le sole operazioni e per i soli scopi ivi previsti; a non comunicare i dati a soggetti diversi da quelli dalle stesse autorizzati ad effettuare le operazioni di trattamento; a non diffondere i dati personali di cui verranno comunque a conoscenza nell'esecuzione del presente Atto, a custodire - in attuazione degli obblighi di riservatezza e di sicurezza imposti dal D. Lgs. 101/2018 e da ogni altra disposizione legislativa o regolamentare in materia - i dati personali saranno trattati in modo tale da evitare rischi di distruzione degli stessi o di accessi a tali dati da parte di soggetti terzi non autorizzati.

E-FIL si impegna ad osservare ed a far osservare, ai propri dipendenti, incaricati e collaboratori, il segreto rispetto a tutti i dati personali dei quali si avrà conoscenza nello svolgimento del servizio e a non diffondere a terzi alcuna informazione o documentazione acquisita in ragione del presente Atto, pena la risoluzione della stessa e relativa assunzione di responsabilità per i danni causati dall'uso improprio.

I dati forniti ad E-FIL, tramite i diversi canali di trasferimento delle informazioni, non dovranno contenere alcun dato classificabile come particolare. E-FIL non effettua controlli in merito, nel caso comunque si evidenziasse la casistica procederà alla cancellazione del dato.

Alla scadenza contrattuale, nel caso di mancato rinnovo, E-FIL procederà alla cancellazione o anonimizzazione dei dati personali ai soli fini contrattuali. Eventuali backup potranno contenere i dati in chiaro per ulteriori 3 mesi.

E-FIL ha definite le regole di mantenimento delle informazioni gestite dal servizio Plug&Pay in modo da ottemperare al principio di trattamento minimo necessario all'esecuzione del servizio, previsto dalla normativa GDPR e al contempo garantire la conformità con le regole di tracciamento dei pagamenti.
La politica aziendale per la sicurezza delle informazioni è pubblicata a: http://www.e-fil.it/wp-content/uploads/2019/07/SI-001-Politica-Sistema-di-Gestione-per-la-Sicurezza-delle-Informazioni.pdf.

4 Certificazioni

E-Fil è dotata delle seguenti certificazioni:

ISO 9001
ISO 27001
ISO 27017 (estensione del sistema di qualità 27001 per il cloud)
ISO 27018 (estensione del sistema di qualità 27001 per la privacy)

Il servizio Plug&Pay è un servizio SaaS qualificato da AgID nel Market Place Cloud PA. La scheda del servizio:
https://catalogocloud.agid.gov.it/service/541