# Certificazione di Compliance PAT

| | |
|---|---|
| Classificazione documento: | Controllato |
| Data Ultimo aggiornamento: | 29/09/2021 |

www.isweb.it

**ISWEB S.p.A.**
Via Cadorna 31 - 67051 Avezzano (AQ)
Via Fiume Giallo 3 - 00144 Roma

**ISO 9001-2015 - RINA**
Sistema di gestione della qualità certificato RINA
Certificato n° 14770/06/S

Numero Verde Gratuito
800 97 34 34

# Indice

# 1. Introduzione

Il presente documento è una autocertificazione delle misure di sicurezza applicate nello sviluppo dei servizi annessi al riuso del software Open Source PAT – Portale Amministrazione Trasparente, soluzione applicativa reperibile sul repository GitHUB dell'AgID (https://github.com/AgID/pat), ed ha lo scopo di certificarne il livello di adeguamento rispetto alle nuove misure di protezione introdotte dal regolamento UE 2016/679, in merito alla privacy dei cittadini della comunità europea.

## 1.1 Contesto applicativo

Il servizio Portale Amministrazione Trasparente consiste in una piattaforma informatica per la gestione e la pubblicazione di un portale dedicato all'Amministrazione Trasparente del committente, strutturato secondo le necessità indicate dal quadro normativo vigente.
La piattaforma informatica utilizzata per il servizio è un software interamente web-based che non necessità l'installazione di alcun componente sul client dell'utilizzatore.

Le tecnologie utilizzate dal servizio nel suo complesso quindi sono:

- Ambiente server basato su LAMP
- Piattaforma CMS (Content Management System) basata su tecnologia PHP
- Componente database basata su MySQL

Il servizio è rivolto a tuti gli utenti che hanno necessità di consultazione delle informazioni o di fruizione di servizi offerti.

## 1.2 Dati trattati e modalità di acquisizione

Il servizio PAT – Portale Amministrazione Trasparente è, per sua natura, dedicato soprattutto alla pubblicazione di informazioni verso l'utenza e minimizza in generale la raccolta di dati sensibili da parte degli utilizzatori.

Nella configurazione standard, non sono presenti moduli di raccolta destinati a dati personali dell'utente, ma solamente le informazioni relative alle utenze amministrative abilitate (nominativo amministratore, indirizzo email, eventuale recapito telefonico).

[Modulo applicativo Accesso Civico]
Nel caso sia stato attivato e configurato il modulo "Accesso Civico", il sistema prevede il trattamento di un modulo di raccolta dati destinato ai facenti richiesta di accesso a specifica documentazione non reperibile in quel momento sul portale.
In questo caso quindi, la piattaforma richiederà i seguenti tipi di dato:

- Nominativo del richiedente
- Codice Fiscale
- Dati di recapito (email, telefono, altro)
- Testo libero di richiesta

[Art. 4 GDPR]
La struttura degli eventuali dati raccolti può variare in funzione delle esigenze del committente, ma in generale anche le possibili variazioni non modificano lo scenario presentato.

[Art. 9 GDPR]
Il servizio non prevede la richiesta o il trattamento di dati appartenenti a categorie particolari, come opinioni sessuali, politiche o religiose.

## 1.3 Dati di navigazione e COOKIE

A scopo di monitoraggio tecnico del servizio, la piattaforma tiene traccia nei log tecnici dell'ambiente server dei seguenti dati relativi all'utilizzo del sistema:

- Indirizzo IP navigatore
- User Agenti
- Orario, tipo e protocollo di richiesta
- Risorsa richiesta
- Tempo e codice della risposta

La piattaforma inoltre fa utilizzo esclusivamente di cookie tecnici per il suo utilizzo, e non utilizza alcun tipo di cookie di profilazione e/o di terze parti.

## 1.4 Data Retention Policy

I tempi di conservazione dei dati trattati all'interno della piattaforma software sono gestiti direttamente dal committente, tramite gli strumenti amministrativi disponibili sulla piattaforma PAT.
Dato l'ambito di applicazione e viste le necessità normative di archiviazione di talune informazioni, la gestione della temporizzazione dei dati è quindi in carico al committente.

I tempi di conservazione dei dati di navigazione, gestiti a livello server, non sono mai superiori ai 2 anni.

## 2. Misure di sicurezza e correttivi per garantire i livelli di sicurezza richiesti

Per il servizio sono stati implementate le seguenti misure di sicurezza al fine di garantire un livello di protezione adeguato al tipo di dati personali che raccoglie, come dichiarati in Sezione 1.

| MISURA DI SICUREZZA | APPLICATA |
|---|---|
| I nostri team di developer hanno seguito le linee guida della OWASP per lo sviluppo di applicazioni Web sicure. | Il servizio PAT – Portale Amministrazione Trasparente è stato sviluppato seguendo le migliori pratiche in merito a:<br>● Sanitizzazione input utente per proteggere le form dell'applicazione da attacchi di tipo XSS;<br>● Sanitizzazione input utente per proteggere l'applicazione da attacchi di tipo Injection;<br>● Aggiornamento regolare del software di terze parti utilizzato per le nostre applicazioni;<br>● Revisione delle configurazioni applicate ai servizi |
| Abbiamo eseguito Vulnerability Assessment/Penetration Test sull'applicazione. | Si, vengono svolte attività di VA periodiche sul software PAT con cadenza almeno annuale.<br>A partire dal 2020, sono disponibili anche analisi svolte da organizzazioni esterne. |
| L'applicazione gode di una protezione conforme alle best practice più aggiornate, nell'archiviazione delle password. | Si, le password memorizzate nel database relativamente alle utenze applicative sono crittografate attraverso funzione di derivazione script. In particolare, si specifica l'utilizzo dell'algoritmo AES a 256bit con applicazione contemporanea di chiave applicativa e chiave singola SALT. Oltre queste applicazioni, ogni credenziale viene crittografata con utilizzo di ulteriore strato crittografico MD5 sia in entrata sia in uscita. |
| Permettiamo l'obbligo di revisione, da parte di un responsabile, dei dati inseriti dall'utente prima di procedere con l'archiviazione definitiva del dato, al fine di agevolare l'azienda cliente nel garantirsi la minimizzazione dei dati. | Non applicabile genericamente dato il contesto applicativo. Nel caso dell'utilizzo delle funzionalità di accesso civico, tutte le informazioni raccolte sono comunque soggette a cicli di workflow definibili dal committente. |
| Garantiamo agli utenti dell'applicazione la possibilità di reperire e aggiornare tutti i dati che lo riguardano, presenti nell'applicazione. | Si, l'operazione di modifica dei dati raccolti è sempre possibile tramite gli strumenti di amministrazione interni a PAT |
| I dati contenuti nelle tabelle dei nostri DB sono crittografati, al fine di proteggerli in caso di furto o fuoriuscita accidentale. | Tutti dati che potrebbero contenere informazioni di stampo personale, come l'accesso civico ed i dati relativi alle utenze applicative, sono |

| | |
|---|---|
| | crittografati tramite AES 128bit con applicazione di duplice chiave (numerica+alfanumerica) |
| I dati in transito da e verso l'applicazione sono protetti da crittografia, per proteggerli in caso di intercettazione. | Si, l'applicazione utilizza correttamente il protocollo SSL per tutte le comunicazioni in entrata ed in uscita |
| Le categorie di dati particolari [Art. 9 GDPR] sono Pseudonimizzati nel momento dell'archiviazione, al fine di proteggere la privacy dell'individuo in caso di furto o fuoriuscita accidentale degli stessi. | Non è normalmente prevista la raccolta di dati appartenenti a categorie particolari. |
| Le categorie di dati particolari [Art. 9 GDPR] vengono classificati nel momento in cui vengono immessi nel nostro software e seguono un flusso totalmente distinto da altri dati personali, allo scopo di poterli identificare facilmente durante il loro percorso e permanenza all'interno dell'applicazione. | Non è prevista la raccolta di dati appartenenti a categorie particolari |

# 3. Conclusioni

## 3.1 Rischio Residuale

Il servizio PAT – Portale Amministrazione Trasparente ha come scopo principale la pubblicazione di informazioni, e le basi dati oggetto di trattamento quindi sono limitate alla richiesta di accesso civico, nel caso sia stato attivato e configurato.

Non è interesse del servizio ottenere informazioni diverse da quelle direttamente richieste.

Nello specifico, le categorie di dati trattati sono quindi relative a:

- Nominativo del richiedente
- Codice Fiscale
- Dati di recapito (email, telefono, altro)
- Testo libero di richiesta

Il rischio residuale è quindi da considerarsi minimo.

## Contatti

**ISWEB S.p.A.**

Azienda certificata UNI EN ISO 9001:2015 - RINA
“Progettazione e sviluppo applicativi software per ambienti di rete”

Sede legale e factory:
Via Cadorna, n.31 - 67051 - Avezzano (AQ)
Unità locale (commerciale):
via Fiume Giallo, 3 - 00144 - Roma

**NUMERO VERDE**
**800.97.34.34**

Tel. +39.0863.441163
Fax. +39.0863.444757

e-mail: info@isweb.it
pec: pec@pec.isweb.it
Sito web: http://www.isweb.it

# Elenco firmatari

*ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI*

Questo documento è stato firmato da:

*NOME: VISINTIN ROBERTO*
*CODICE FISCALE: VSNRRT69E24Z133P*
*DATA FIRMA: 13/06/2022 12:27:45*
*IMPRONTA: 5537E76BF8776B7DD06B1D099B40F009B128409196A1E0C8AF29E92EE5933E98*
*B128409196A1E0C8AF29E92EE5933E98ECD39DBB929DAC28942F2F8EB4FD77B9*
*ECD39DBB929DAC28942F2F8EB4FD77B9E32ADA4590F648A337A1292103A13350*
*E32ADA4590F648A337A1292103A133501015E1063BBB3870F21C5B7BAA996D2D*