ACARA Privacy and Security Whitepaper

Prima revisione, gennaio 2023

INDICE DEGLI ARGOMENTI

1. PERCHÉ ACARA 2
1.1 CHI SIAMO 2
1.2 PRIVACY & SECURITY BY DESIGN 2
1.3 METODOLOGIA DI SVILUPPO 2
2. LA SICUREZZA DI ACARA 3
2.1 SEPARAZIONE DEI DATI 3
2.2 COME PROTEGGIAMO I DATABASE 3
2.3 COME PROTEGGIAMO I DATI IN TRANSITO 3
2.4 COME PROTEGGIAMO LE PAGINE PUBBLICHE 4
2.5 INFRASTRUTTURA ICT E MONITORAGGIO ANOMALIE 4
2.6 AUTENTICAZIONE 4
2.7 LOG DI SISTEMA 4
3. TRATTAMENTO DATI E RUOLI 5
3.1 COSA SI INTENDE PER SEGNALAZIONE ANONIMA 5
3.2 COME PROTEGGIAMO L'IDENTITÀ DEL SEGNALANTE 5
3.3 DATI PERSONALI TRATTATI DALLA PIATTAFORMA 6
3.4 TIPOLOGIE DI CAMPI SEGNALAZIONE 6
3.5 TRASPARENZA 7
3.6 PROFILI UTENTE E ASSEGNAZIONE DEI RUOLI 7
4. RUOLI DEL TRATTAMENTO 8
4.1 LA FILIERA DEI DATI 8
4.2 DATA PROCESSING AGREEMENT 8
4.3 ASSISTENZA AL CLIENTE 8

1. PERCHÉ ACARA

Acara è un termine **sanscrito** che significa 'guida', 'disciplina' o 'vita quotidiana'. Con lo stesso termine si indicano anche le norme consuetudinarie dell'Hinduismo, cioè quelle regole non necessariamente scritte che però regolano la vita di tutti i giorni e i rapporti con le persone.

È con questa filosofia che abbiamo voluto sviluppare una piattaforma per le segnalazioni che potesse anche essere uno strumento per aiutare le aziende a mantenere una **cultura fondata sulla legalità** e sul rispetto delle regole – anche di buona convivenza. Per farlo, è però fondamentale avere uno strumento che possa **proteggere le persone** che espongono se stesse per segnalare comportamenti illeciti come corruzione, mobbing e molestie sessuali, o violazioni di dati personali.

1.1 CHI SIAMO

Acara nasce dall'esperienza di **Net Patrol Italia** nel campo della **privacy**, **cybersecurity** e della **compliance**. Dal 2018 aiutiamo aziende in settori complessi come quello delle telecomunicazioni, dell'energia, della GDO o della sanità ad affrontare le sfide del digitale e della protezione dei patrimoni informativi.

Il nostro team è composto da figure professionali eterogenee, come giuristi, ethical hacker, esperti di cybersecurity e protezione delle infrastrutture critiche, tecnici informatici e sviluppatori software.

1.2 PRIVACY & SECURITY BY DESIGN

Proteggere l'identità di chi vuole segnalare abusi e violazioni di legge richiede un approccio incentrato sulla privacy & security by design. Fin dalle prime fasi di progettazione, Acara è stato immaginato e sviluppato secondo rigorosi requisiti mutuati dalla **normativa privacy europea** ("GDPR") e dai migliori standard nel campo della **sicurezza delle informazioni**. Sono questi requisiti che hanno plasmato poi tutte le altre funzionalità di Acara, fino a creare un prodotto che poggia la sua intera struttura su solide fondamenta di privacy e sicurezza dei dati.

1.3 METODOLOGIA DI SVILUPPO

Acara è stata sviluppata tenendo conto di tutti i **principi e requisiti delle normativa** per la protezione dei dati (Reg. UE 2016/679), così come le normative in materia di responsabilità amministrativa da reato e whistleblowing (D.Lgs 231/2001, Dir. UE 2019/1937) e gli standard ISO 37001:2016.

Durante lo sviluppo, sono stati centrali i seguenti parametri:

Trasparenza	Attenzione ai **flussi di dati** e ai **soggetti coinvolti**, per assicurare che tutti gli stakeholder abbiano a disposizione tutte le informazioni necessarie per capire il funzionamento della piattaforma e i dati trattati.
Controllo	Attenzione alle possibilità di intervento sui campi della segnalazione e dei ruoli, garantendo il **controllo totale** degli stessi da parte dell'azienda.
Minimizzazione	Attenzione alle tipologie di dati acquisiti e alle modalità di gestione delle segnalazioni, con particolare riguardo ai privilegi di accesso e misure per **limitare l'uso dei dati** e la loro conservazione nel tempo.
Sicurezza	Attenzione alla **sicurezza dei sistemi informativi** necessari al funzionamento della piattaforma e alla sicurezza dei dati, attraverso l'uso estensivo di crittografia e segmentazione dei database.

2. LA SICUREZZA DI ACARA

Tenuto conto del particolare campo di applicazione, Acara è stato sviluppato per raggiungere questi obiettivi primari:

- Sicurezza e crittografia dei dati, sia in transito che a riposo
- Protezione totale dell'identità dei segnalanti
- Accountability e trasparenza
- Piena libertà di configurazione di ogni aspetto della piattaforma da parte dell'azienda

2.1 SEPARAZIONE DEI DATI

Il database dell'applicativo è stato pensato nel rispetto dei **principi di minimizzazione e sicurezza by design**. Per farlo, abbiamo strutturato i database in modo da archiviare separatamente i diversi elementi di una segnalazione:

- Testo e codice della segnalazione
- Campi aggiuntivi *non identificativi*
- Campi aggiuntivi *potenzialmente identificativi*

In questo modo garantiamo un layer aggiuntivo di sicurezza e minimizzazione, evitando così di accentrare i dati in un unico database.

2.2 COME PROTEGGIAMO I DATABASE

Sappiamo che le segnalazioni possono contenere informazioni e documenti molto sensibili, specie nelle segnalazioni di reati particolarmente gravi come corruzione o molestie sessuali. Per questo abbiamo scelto di cifrare l'intero database dell'applicativo.

La tecnologia scelta per la realizzazione della base dati è **Amazon Aurora**, che permette la gestione di database relazionali e consente di crittografare i database usando le chiavi create e gestite mediante **AWS Key Management Service** (AWS KMS).

In ogni istanza database in esecuzione con crittografia di Amazon Aurora i dati a riposo sono crittografati, così come i **backup** automatici, gli **snapshot** e le **repliche** incluse nello stesso cluster. Il servizio usa una tecnologia denominata "envelope encryption", garantita dall'AWS KMS. L'envelope encryption è la pratica con la quale si procede a **crittografare a loro volta le chiavi di crittografia** utilizzate per proteggere i dati. AWS KMS permette di proteggere con moduli di sicurezza hardware le chiavi dati di crittografia, archiviandole in modo sicuro.

Tramite queste procedure viene garantita la **riservatezza dei dati** anche nel caso di accesso al sistema effettuato dal responsabile IT della piattaforma per le operazioni di manutenzione e assistenza.

2.3 COME PROTEGGIAMO I DATI IN TRANSITO

I dati in transito sono protetti grazie a **protocolli di crittografia** SSL/TLS. Oltre a questi layer di protezione a livello applicativo, usiamo inoltre connessioni HTTPS per i servizi di frontiera (tra client e server), per garantire che tutti i dati in transito siano adeguatamente protetti.

2.4 COME PROTEGGIAMO LE PAGINE PUBBLICHE

Per proteggere le pagine pubbliche del centro segnalazioni aziendale da attacchi di bot automatici e utilizzi malevoli dei moduli, l'applicativo usa il sistema Captcha AWS WAF CAPTCHA.

Inoltre, grazie all'uso del filtro ***HttpHeaderSecurityFilter*** di Apache Tomcat l'applicativo potrà garantire un maggior grado di sicurezza per ogni pagina pubbliche. Il filtro fornisce infatti un meccanismo per aggiungere i seguenti header http definiti dagli standard di sicurezza OWASP Secure Headers Project:

- **HTTP Strict Transport Security (HSTS)** tramite il quale il server può dichiarare al browser che deve interagire solo utilizzando connessioni HTTPS;
- **X-Frame-Options (denominata anche XFO)** che migliora la protezione dell'applicazione contro il clickjacking. Tale intestazione indica al browser se il contenuto può essere visualizzato all'interno di frame;
- **X-Content-Type-Options** che viene impostata su ogni risposta per bloccare lo sniffing del tipo di contenuto;
- **X-XSS-Protection: 1** che viene impostata su ogni risposta per abilitare la protezione del filtro di cross-site scripting del browser.

L'applicativo è inoltre configurato per rendere accessibili i cookie di sessione solo tramite https – per prevenire eventuali manipolazioni.

2.5 INFRASTRUTTURA ICT E MONITORAGGIO ANOMALIE

L'applicativo è dotato di un sistema di monitoraggio delle **azioni potenzialmente malevole**, come: tentativi di login eccessivi, modifica delle credenziali utente, accesso a risorse private in modo anomalo. Il sistema produce una reportistica periodica con **indicazione dell'indirizzo IP** che ha effettuato le azioni.

L'applicativo è sviluppato su infrastrutture AWS, esclusivamente su **Region UE.** Le soluzioni scelte garantiscono la conformità a tutte le principali certificazioni di sicurezza e affidabilità: **ISO 27001**, **ISO 22301**, **ISO 27701**, **SOC 1**, **SOC 2** e **SOC 3**.

L'architettura è strutturata per garantire la massima affidabilità e resilienza, oltre ad essere monitorata 24 ore al giorno e 7 giorni su 7 sia per quanto riguarda l'uptime che per la latenza.

L'applicativo viene periodicamente sottoposto a verifica di sicurezza con attività di Vulnerability Assessment e vengono rilasciati dal team di sviluppo aggiornamenti periodici di sicurezza.

2.6 AUTENTICAZIONE

Ogni operatore incaricato di gestire le segnalazioni può accedere alla piattaforma esclusivamente previa **autenticazione** tramite utente e password univoche.

La piattaforma adotta degli standard minimi di complessità delle password, che devono essere rispettati obbligatoriamente. Le password degli utenti sono conservate in modo sicuro attraverso l'implementazione di **algoritmi di hashing** (cifratura) che le rendono illegibili sia dagli amministratori di sistema che da attaccanti esterni.

2.7 LOG DI SISTEMA

L'intera infrastruttura è sottoposta a processi di **auditing e logging** per il monitoraggio e il tracciamento di tutti gli eventi di sicurezza. Usiamo questi processi per assicurare la compliance normativa e per garantire un'adeguata visibilità e verificabilità degli eventi umani e non, per eventuali investigazioni in caso di incidenti.

3. TRATTAMENTO DATI E RUOLI

3.1 COSA SI INTENDE PER SEGNALAZIONE ANONIMA

Acara è stato progettato offrire alle aziende la possibilità di scegliere se identificare i segnalanti o se invece proteggere il loro anonimato, nel rispetto degli **standard ISO ISO 37001:2016** (Sistemi di gestione per la prevenzione della corruzione) e come previsto anche dalla **normativa europea sul Whistleblowing** (Dir. UE 2019/1937).

Su questo punto, merita però evidenziare che secondo gli standard accettati a livello internazionale, come la **ISO 29100**, un dataset si può considerare anonimo solo nel momento in cui le informazioni personali identificabili (dati personali) siano modificate in modo tale che una persona fisica **non possa più essere identificata direttamente o indirettamente**, né dal titolare né da altri.

L'efficacia dell'anonimizzazione dipende dall'assenza di tre elementi:

- **Single-out / individuabilità**: è possibile isolare alcuni dati che identifificano una persona all'interno di un insieme di dati
- **Linkability / correlazione**: è possibile collegare alcuni dati concernenti la stessa persona o gruppo di persone
- **Inference / deducibilità**: è possibile desumere con un alto grado di probabilità il valore di un attributo partendo da un insieme di altri attributi

La stessa Direttiva europea 2019/1937 utilizza impropriamente il termine "segnalazioni anonime", affermando infatti all'articolo 6 che *"Le persone che hanno segnalato o divulgato pubblicamente informazioni su violazioni **in forma anonima**, ma che **successivamente sono state identificate** e hanno subito ritorsioni, possono nondimeno beneficiare della protezione prevista ai sensi del capo VI, a condizione che soddisfino le condizioni di cui al paragrafo 1".*

Considerando il concetto di "dataset anonimo" di cui agli standard citati, e considerando l'articolo qui richiamato, parrebbe il legislatore europeo intenda riferirsi piuttosto alla circostanza di nascondere e proteggere l'identità del segnalante, che non sarebbe immediatamente e facilmente conoscibile dall'azienda.

Non riteniamo però che il mero uso di un software come Acara possa essere sufficiente a **garantire vero e assoluto anonimato** del segnalante, poiché deve essere valutato il contesto aziendale, l'infrastruttura informatica e il trattamento di dati nel suo insieme. Non soltanto, dunque, la fase riguardante la segnalazione.

È infatti possibile che in determinati contesti un segnalante possa essere comunque identificabile in base a informazioni acquisite proprio grazie alla segnalazione (ad esempio la descrizione di alcuni avvenimenti). Si consiglia pertanto di fare attenzione al contesto aziendale e di tenere in considerazione che il **Reg. UE 2016/679** (**GDPR**) si applica anche al trattamento di dati dei soggetti segnalanti.

3.2 COME PROTEGGIAMO L'IDENTITÀ DEL SEGNALANTE

La piattaforma Acara è stata pensata e costruita per proteggere il più possibile l'identità del segnalante e per rendere ardua la sua identificazione.

Per inviare una segnalazione i dipendenti (o altri stakeholder) avranno a disposizione una pagina pubblica, che non richiederà alcun tipo di autenticazione o riconoscimento. In questa pagina il segnalante potrà compilare i vari campi della segnalazione.

Una volta inviata la segnalazione, l'utente riceverà **un codice alfanumerico univoco** composto da 16 cifre.

Solo tramite questo codice il segnalante potrà accedere successivamente alla sua segnalazione per verificarne lo stato di avanzamento.

Il sistema è progettato in modo tale da **non raccogliere alcun dato identificativo**, se non esplicitamente richiesto dall'azienda. Nei casi in cui l'azienda richieda la compilazione di campi che potrebbero contenere dati identificativi, abbiamo comunque previsto la possibilità di **nascondere *di default*** i dati identificativi agli operatori, in base al profilo assegnato.

3.3 DATI PERSONALI TRATTATI DALLA PIATTAFORMA

Attraverso la piattaforma Acara possono essere acquisiti le seguenti tipologie di dati personali:

	Dati di contatto e credenziali di accesso	Gli admin e gli operatori accedono alla piattaforma tramite autenticazione, per questo è necessario trattare questa tipologia di dati
	Dati contenuti nei campi delle segnalazioni	Alcuni campi delle segnalazioni possono contenere dati personali dai quali potrebbe essere possibile l'identificazione del segnalante e delle persone coinvolte. Attraverso la piattaforma è inoltre possibile allegare documenti e file che potrebbero contenere dati personali a loro volta.
	IP e log di sistema	La piattaforma acquisisce gli indirizzi IP degli utenti in caso di azioni anomale, come descritto nella sezione 3. Il sistema crea inoltre log di sistema che descrivono le azioni effettuate dagli operatori, per garantire trasparenza e un audit trail nel caso in cui ciò sia necessario per ricostruire eventuali violazioni di sicurezza o errori nella gestione delle segnalazioni. I log contengono i seguenti dati: utente, data, IP, azione effettuata.

3.4 TIPOLOGIE DI CAMPI SEGNALAZIONE

L'azienda ha completa libertà di scelta nella creazione dei campi di una segnalazione, secondo formati diversi come testi, elenchi numerici, date, o campi a risposta multipla.

Ogni campo può ulteriormente essere personalizzato in base alle sue caratteristiche e contenuto potenziale:

	Campi obbligatori	Sono i campi che devono essere obbligatoriamente compilati per poter inviare una segnalazione.

	Campi facoltativi	Sono i campi che l'azienda ritiene importanti ma che per diversi motivi non risultano obbligatori per poter inviare una segnalazione.
	Campi identificativi	Sono i campi che potrebbero contenere dati direttamente identificativi, come nomi e cognomi, oppure dati indirettamente identificativi, come la descrizione di avvenimenti specifici. I campi identificativi possono essere obbligatori o facoltativi.
	Allegati	Ogni segnalazione permette di allegare file e documenti. Gli allegati sono facoltativi e potrebbero contenere dati personali.

3.5 TRASPARENZA

Per agevolare la comunicazione delle informazioni relative al trattamento dati realizzato con Acara, abbiamo preparato un **modello di privacy policy** che viene fornito al cliente.

Il modello deve essere integrato e/o revisionato dall'azienda, per accertare che siano incluse tutte le informazioni di dettaglio che si rendano necessarie, tenuto conto dello specifico trattamento di dati nel suo insieme. Consigliamo comunque di aggiornare le informazioni almeno ad ogni modifica dei campi della segnalazione, in special modo se la modifica comporta il trattamento di nuovi e/o ulteriori dati personali.

3.6 PROFILI UTENTE E ASSEGNAZIONE DEI RUOLI

Ogni azienda ha a disposizione quattro ruoli diversi che possono essere assegnati ai diversi operatori. Ognuno di questi profili ha privilegi di accesso differenziati a seconda della funzione ricoperta, nel rispetto del **principio di minimo privilegio**.

	Admin	L'admin è il ruolo che permette la creazione e la gestione di altri ruoli. L'admin può inoltre modificare i campi richiesti per le segnalazioni, modificare la privacy policy e ogni altro aspetto configurabile della piattaforma.
	Operatore account	L'operatore account è il ruolo che permette la creazione e la gestione di altre utenze e l'assegnazione dei rispettivi ruoli.
	Custode delle identità	Il custode delle identità è il ruolo che permette di assegnare la gestione dei dati identificativi di ogni segnalazione a un soggetto separato rispetto agli operatori. Può autorizzare o meno la visualizzazione di questi dati su richiesta motivata dell'operatore che ha in carico la segnalazione.
	Operatore segnalazioni	L'operatore segnalazioni è il ruolo che permette la gestione delle segnalazioni pervenute tramite la piattaforma. L'operatore non visualizza di default i campi identificativi e per farlo deve richiedere autorizzazione al custode delle identità.
	Responsabile segnalazioni	Il responsabile segnalazioni è il ruolo che oltre a permettere la gestioen delle segnalazioni pervenute tramite la piattaforma consente anche di visualizzare by default tutti i campi, compresi quelli potenzialmente identificativi. È un ruolo totalmente autonomo che sacrifica il principio di minimizzazione per favorire le realtà che non sono strutturate per avere un alto livello di segmentazione dei ruoli.

4. RUOLI DEL TRATTAMENTO

4.1 LA FILIERA DEI DATI

L'azienda che acquista e utilizza Acara acquisisce il ruolo di **Titolare del trattamento** per tutto ciò che riguarda il trattamento di dati realizzato attraverso la piattaforma – dal momento dell'acquisizione dei dati contenuti in una segnalazione, fino alla loro cancellazione.

La piattaforma viene fornita in modalità *"Software as a Service"* (SaaS) da Net Patrol Italia, che contestualmente tratta dati personali per conto dell'azienda cliente. Per questo, Net Patrol Italia è qualificabile come **Responsabile del trattamento.**

Per garantire il funzionamento della piattaforma e l'assistenza ai clienti, abbiamo bisogno anche del supporto di alcuni **fornitori ICT specializzati**, che saranno qualificati come sub-responsabili del trattamento.

Il cliente avrà a disposizione un **elenco dei sub-responsabili e delle loro attività** nel Data Processing Agreement. Sarà nostra cura notificare con congruo anticipo ogni successiva modifica degli stessi.

4.2 DATA PROCESSING AGREEMENT

Il trattamento di dati realizzato da Net Patrol Italia per conto dei clienti che scelgono Acara è regolato da uno specifico ***Data Processing Agreement***, allegato alle condizioni generali di contratto.

Il Data Processing Agreement disciplina in modo dettagliato **obblighi e diritti** del Titolare del trattamento e del Responsabile del trattamento, così come le modalità di svolgimento del trattamento di dati e ogni garanzia richiesta dalla legge.

4.3 ASSISTENZA AL CLIENTE

Siamo consapevoli dell'importanza del ruolo di Responsabile del trattamento. Per questo motivo, abbiamo adottato un **sistema di gestione** che ci permette di **assistere le aziende clienti** per qualsiasi questione inerente al trattamento dei dati personali realizzato con Acara.

In particolare, ci impegnamo ad assistere tecnicamente il cliente e fornire ogni informazione aggiuntiva per soddisfare i seguenti adempimenti previsti dal Reg. UE 2016/679 (GDPR):

	Articoli 15-22	Ci impegniamo ad assistere i clienti per garantire un riscontro adeguato ed entro i termini di legge per ogni richiesta di **esercizio dei diritti previsti dal GDPR** (accesso, portabilità, modifica, cancellazione, limitazione). Nota: l'articolo 22 non trova applicazione in questo contesto.
	Articolo 35	Le informazioni contenute in questo Whitepaper dovrebbero essere sufficienti per aiutare il cliente a svolgere una **valutazione d'impatto** preventiva. In ogni caso, siamo disponibili ad offrire assistenza e ulteriori informazioni specifiche nel caso in cui ciò sia necessario.
	Articoli 33-34	In caso di **violazione di dati** il nostro team di sicurezza condividerà tempestivamente ogni informazione necessaria per valutare l'incidente e, se del caso, notificarlo alle Autorità competenti e ai soggetti interessati.

NET PATROL ITALIA

Competenti nel proteggere

www.netpatrol.it

Acara è un prodotto Net Patrol Italia, società specializzata in privacy, cybersecurity e digital compliance. Il business partner che protegge il futuro digitale della tua azienda.

info@netpatrol.it - 02 87165913

Milano
Via Napo Torriani, 31

Udine
Via Molin Nuovo, 37/38

ACARA