

Progetto Antifrode

Documento di sintesi

Struttura ed obiettivi del Progetto antifrode

Con il progetto illustrato nel presente documento (il "Progetto") l'ANIA si pone come obiettivo quello di supportare le Compagnie assicurative (le "Compagnie"), gli Organi Giudiziari e le Autorità di vigilanza nello svolgimento delle attività antifrode.

A tal fine l'ANIA ha elaborato:

- una **Piattaforma antifrode** (la "Piattaforma") che consente di raccogliere informazioni anonimizzate sui diversi macrofenomeni fraudolenti osservati dalle imprese nel corso della propria attività antifrode, con l'obiettivo di fungere da strumento d'ausilio per la valutazione dell'andamento delle diverse tipologie di fenomeni fraudolenti e della loro distribuzione sul territorio
- un **Portale Antifrode** non auto (il "Portale"), che rappresenta uno strumento di consultazione dei sinistri utilizzabile tanto dalle Compagnie in fase liquidativa, che dalle Autorità Giudiziarie e dalle Autorità di Vigilanza, quale ad esempio IVASS, per lo svolgimento delle attività investigative e ispettive

Tali strumenti oltre ad essere degli efficaci mezzi di contrasto (e prevenzione) delle frodi sono in grado di migliorare l'efficienza dell'intero sistema, consentendo: i) ingenti risparmi in termini di tempi e di costi per le Compagnie (per i sinistri a potenziale rischio frode); ii) benefici a valle per gli assicurati, sia in termini riduzione dei costi delle polizze, conseguente alla riduzione delle «mutualità negative» sia in termini di maggiore velocità nella liquidazione dei sinistri che non presentano fattori di criticità; iii) rilevanti risparmi dal punto di vista delle spese di giustizia (a carico di tutti i soggetti, inclusi quelli pubblici) connesse ai fenomeni di frode; iv) una più efficace attività di monitoraggio e individuazione di fenomeni associativi da parte delle Autorità competenti.

La Piattaforma antifrode

Caratteristiche della Piattaforma



La Piattaforma opera in relazione a **tutti i rami assicurativi** menzionati dal Codice delle Assicurazioni Private (art.2)



La struttura e il contenuto **escludono il trattamento di dati personali o sensibili**: i dati scambiati riguardano informazioni che non possono essere collegate a soggetti identificati o identificabili.



Lo strumento consente di **raccogliere informazioni sui diversi macro fenomeni fraudolenti** osservati dalle imprese nel corso della propria attività antifrode, con l'obiettivo di **segnalare gli schemi di frode ricorrenti al fine di far emergere situazioni di rischio per il corretto svolgimento delle attività di liquidazione dei sinistri, nonché reati di tipo associativo.**



Le **informazioni** vengono inserite nei campi sulla base di una serie di **elenchi predefiniti** (c.d. elenchi chiusi o vincolati); sono previsti anche **campi non vincolati facoltativi** in cui è **fatto divieto alle imprese di riportare dati sensibili o a carattere commerciale** (*per maggiori dettagli si rimanda alle pagine che seguono*).



I record sono compilati dalle Compagnie con **l'indicazione** (non di un singolo sinistro, ma) **di una fattispecie fraudolenta riscontrata**.

Tutte le informazioni caricate (ad eccezione del nome della Compagnia che effettua il caricamento) sono visualizzabili in modalità sola lettura; inoltre, sul **Dashboard** sono visibili le elaborazioni grafiche realizzate da ANIA sulla base delle informazioni caricate.

Soggetti abilitati all'accesso

Associate ANIA

- La Piattaforma è stata realizzata con le risorse provenienti dalla contribuzione ordinaria e dunque con risorse degli Associati
- Pertanto, tali Compagnie potranno accedere alla Piattaforma senza versare alcun ulteriore contributo

Non Associate ANIA

- Le Compagnie assicurative non associate ad ANIA avranno la possibilità di accedere alla Piattaforma **corrispondendo un contributo che sarà quantificato nel rispetto dei principi di parità di trattamento e non discriminazione** rispetto a quanto versato dalle associate
- I contenuti resi accessibili alle Compagnie non associate saranno **i medesimi visualizzabili dalle associate**

Soggetti Istituzionali

- I soggetti istituzionali (a titolo esemplificativo, IVASS, Procure della Repubblica, Polizia di Stato, Arma dei Carabinieri e Guardia di Finanza) avranno accesso a **titolo gratuito** alla Piattaforma
- A tali soggetti sarà garantito accesso integrale a **tutte le informazioni contenute sulla Piattaforma**.

Convenzione per l'utilizzo della Piattaforma: elementi essenziali

- L'accesso alla Piattaforma viene disciplinato da una apposita Convenzione tra ANIA e le singole Compagnie, che le imprese dovranno formalmente approvare e sottoscrivere per poter utilizzare la Piattaforma
- La Convenzione indica anche:
 - Le **finalità** per cui è consentito l'accesso alla Piattaforma, ossia esclusivamente per l'individuazione dei macrofenomeni ricorrenti e la valutazione della loro distribuzione sul territorio, così da contrastare in maniera più efficace le frodi in ambito assicurativo e individuare possibili reati di tipo associativo
 - L'elenco dei **soggetti abilitati** a consultare la Piattaforma, in cui rientrano (a prescindere dalla qualifica di Associati all'ANIA): *i)* le imprese di assicurazione italiane autorizzate all'esercizio nel territorio della Repubblica e che abbiano dei sinistri da liquidare sul territorio nazionale; *ii)* le imprese di assicurazione dell'Unione europea e a quelle aderenti allo Spazio economico europeo abilitate all'esercizio nel territorio della Repubblica dell'attività assicurativa in regime di libertà di prestazione di servizi o in regime di stabilimento e che abbiano sinistri da liquidare sul territorio nazionale; *iii)* le imprese che svolgono attività liquidativa dei sinistri in nome e per conto dell'impresa di assicurazione (laddove quest'ultima non vi aderisca direttamente), e che abbiano sinistri da liquidare sul territorio nazionale
 - L'elenco degli **obblighi** cui sono soggetti gli utenti che comprenderanno, in via esemplificativa: i) utilizzare le informazioni contenute sulla Piattaforma esclusivamente per finalità antifrode; ii) attenersi alle indicazioni e alle modalità operative riportate nel **Manuale di utilizzo della Piattaforma**, che costituisce parte integrante della Convenzione iii) dotarsi, a proprie spese, dell'hardware necessario, di infrastruttura di rete e software per accedere al Portale; iv) fornire informazioni complete sui soggetti autorizzati ad accedere al Portale ed ogni aggiornamento dei soggetti abilitati; v) porre in essere tutte le attività necessarie per prevenire e/o eliminare eventuali operazioni fraudolente, adottando la massima diligenza; vi) non cedere a terzi, a titolo gratuito od oneroso, le informazioni acquisite tramite il Portale.
 - La possibilità per ANIA di **eseguire controlli** sull'utilizzo del Piattaforma, disponendo, in caso di reiterate violazioni degli obblighi da parte degli utenti, la sospensione temporanea o la disabilitazione definitiva l'utenza

Funzionamento della Piattaforma

Struttura della Piattaforma



Login

Pagina di login della Piattaforma web in cui ogni impresa inserisce le proprie credenziali per accedere



Input sheet

Maschera di input in cui le imprese inseriscono le informazioni richieste per la mappatura dei fenomeni fraudolenti, sulla base di elenchi predefiniti (v. All. 1)



Analysis sheet

Raccolta delle informazioni messe a disposizione dalle imprese, accessibile in consultazione. I soli record inseriti dall'impresa che consulta la Piattaforma saranno identificabili attraverso uno specifico riferimento. I record inseriti dalle altre compagnie non avranno riferimenti che consentano di risalire alla Compagnia che ha caricato il dato.



Dashboard

Contiene una serie di elaborazioni grafiche con la possibilità di selezionare i filtri (basati sui campi di input) che le imprese ritengono più funzionali alle proprie analisi. Le statistiche si aggiornano in tempo reale ad ogni inserimento di nuove segnalazioni da parte delle imprese aderenti alla Piattaforma.

Funzionamento della Piattaforma

Logiche di gestione

 Da un **punto di vista tecnologico**, la Piattaforma è stata sviluppata in *excel* con l'utilizzo di macro in linguaggio VBA e si basa sulla seguente **logica di gestione**:

 **Condivisione** in cloud sul file hosting "box", ad accesso protetto, dei **file** relativi alle singole **imprese associate**.

 **Accesso** delle imprese alla Piattaforma previa autenticazione con **username** e **password** attribuiti alle singole associate:

-  sia per **alimentare** la Piattaforma con i fenomeni fraudolenti osservati;
-  sia per **consultare**, in modalità lettura, i fenomeni aggregati e le analisi statistiche preimpostate.

Funzionamento della Piattaforma

Output: Informazioni aggregate


 Le imprese avranno accesso all'insieme delle **informazioni aggregate** sui macro fenomeni fraudolenti osservati nel corso della loro operatività. I dati sono anonimizzati e non sarà comunque visibile alla Compagnia l'informazione in merito all'Impresa che ha effettuato il caricamento

 L'**accesso alla tabella di output è consentito nel continuo** con le **informazioni** nel database che **si aggiornano in tempo reale** ad ogni inserimento di nuove segnalazioni da parte delle imprese aderenti alla Piattaforma.

Funzionamento della Piattaforma

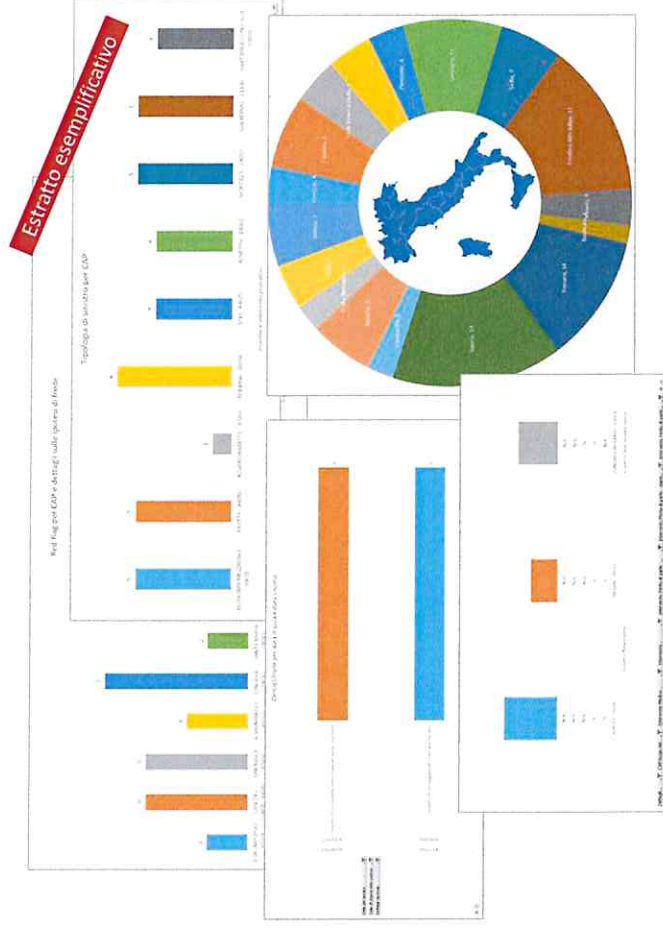
Output: Dashboard

 Le imprese attraverso la «**dashboard**» contenente una serie di **filtri preimpostati** possono visualizzare specifiche **analisi statistiche basate sui dati aggregati**.



DETTAGLIO ANALISI DASHBOARD

- Dettagli frode per Regione, Provincia, Ramo, Red Flag
- Red flag: iniziative legali in fase penale
- Tipologia di sinistro per CAP
- Red flag per CAP e dettagli sulle ipotesi di frode
- Dettagli frode per CAP con evidenza dell'intervento di legale di parte, medico legale di parte, perito di parte
- Lesioni sospette derivanti da fenomeni medico legali e da RCA con relative Red Flag
- Red flag dei fenomeni medico legali per provincia



Misure di sicurezza e di segregazione delle informazioni

- **Limitazione dei soggetti che possono accedere alla Piattaforma per conto delle Compagnie** aderenti alla Piattaforma: le credenziali per l'accesso alla Piattaforma in fase sia di caricamento che di visualizzazione delle informazioni saranno fornite unicamente al Responsabile dell'Ufficio antifrode della singola Compagnia e potranno essere utilizzate unicamente da tale Ufficio, sotto la supervisione del Responsabile antifrode
- In fase di consultazione della Piattaforma **alle Compagnie** (ma non alle Autorità pubbliche) sarà inibita la visualizzazione del **nominativo delle Compagnie che hanno inserito le informazioni** (il sistema consentirà unicamente l'identificazione dei report inseriti dalla Compagnia che effettua l'accesso alla Piattaforma)
- In fase di consultazione delle Piattaforma saranno **disabilitate le funzioni «copia e incolla» e non sarà possibile stampare i risultati** dell'interrogazione.

Il Portale Antifrode Non Auto

Fondamento giuridico del Portale (1)

- Il fenomeno fraudolento ha implicazioni che vanno al di là dello specifico atto di frode, essendo spesso parte di fenomeni criminali a carattere associativo. La diffusione di tali fenomeni può comportare una generale perdita di fiducia nel sistema economico.
- La reazione contro il fenomeno fraudolento ha visto l'Unione Europea intervenire in diversi settori economici della sfera pubblica e della sfera privata, cercando di regolare e disciplinare una serie di misure preventive, deflattive e sanzionatorie delle condotte fraudolente che mirano senz'altro alla tutela del bene privatistico d'interesse della singola impresa, o meglio del gruppo di imprese, ma anche alla protezione della collettività che direttamente o indirettamente risulta afflitta e colpita dalle condotte fraudolente: il Trattato sul Funzionamento dell'Unione Europea ha previsto l'istituzione di uffici *ad hoc* ed in particolare l'Ufficio europeo per la lotta antifrode (c.d. **OLAF**), volto proprio al contrasto dei fenomeni fraudolenti
- Analisi e riscontri dalle Autorità giudiziarie hanno evidenziato la necessità di strumenti efficienti ed efficaci per contrastare il fenomeno delle frodi, che troppo spesso alimentano e sovvenzionano associazioni criminali organizzate (mafia, camorra, droga, terrorismo etc.)

Fondamento giuridico del Portale (2)

- In Italia, due settori sono stati considerati particolarmente esposti a rischio frode, quello bancario e quello assicurativo:
 - a) Decreto legislativo del 11 aprile 2011 n. 64 contenente ulteriori modifiche ed integrazioni al decreto legislativo 13 agosto 2010, n. 141, per l'istituzione di un sistema di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo, con specifico riferimento al furto d'identità
 - b) Codice delle Assicurazioni Private (artt. 134, 135 e 148 e art. 21 decreto-legge 179/2012, convertito in legge 221/2012)
 - c) Art. 642 del Codice penale (la frode assicurativa). Il diritto penale contribuisce ad assicurare condizioni essenziali della convivenza civile, predisponendo la sanzione più drastica a tutela dei beni socialmente considerati, in ragione della loro importanza, meritevoli di protezione giuridico-penale, rappresentando una esigenza di tutela e salvaguardia di un interesse sociale e collettivo
 - d) art. 2-octies del D.lgs. 196/2003 che attribuisce alla prevenzione delle frodi una specifica rilevanza, consentendo il trattamento di dati relativi a condanne penali e reati o a misure di sicurezza laddove esso sia autorizzato da un atto normativo e riguardi, in particolare, *“la prevenzione, l'accertamento il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa”*
 - e) cons. 47 del GDPR che nel fornire taluni parametri interpretativi utili alla valutazione che il titolare dovrà condurre in ordine alla sussistenza del legittimo interesse, espressamente considera la prevenzione delle frodi come un interesse legittimo perseguito dal titolare o da terzi, naturalmente previo test di bilanciamento

Legittimo Interesse anche a fronte di un test di bilanciamento secondo il Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE emanato dal Gruppo di lavoro “Articolo 29 nel 2014.

Caratteristiche del Portale (alla luce degli impegni)

- Il Portale sarà accessibile - oltre che ai soggetti istituzionali - a condizioni eque e non discriminatorie, anche alle Compagnie non associate ad ANIA che abbiano aderito al Codice di Condotta (ex art. 40 del GDPR).
- Nello specifico, l'adesione sarà consentita:
 - alle imprese di assicurazione italiane autorizzate all'esercizio nel territorio della Repubblica e che abbiano dei sinistri da liquidare sul territorio nazionale;
 - alle imprese di assicurazione dell'Unione europea ed a quelle aderenti allo Spazio economico europeo abilitate all'esercizio nel territorio della Repubblica dell'attività assicurativa in regime di libertà di prestazione di servizi o in regime di stabilimento e che abbiano sinistri da liquidare sul territorio nazionale.
 - alle imprese che svolgono attività liquidativa dei sinistri in nome e per conto dell'impresa di assicurazione (laddove quest'ultima non vi aderisca direttamente), e che abbiano sinistri da liquidare sul territorio nazionale;
- Il suo utilizzo sarà disciplinato da un Regolamento ad hoc, applicabile a tutti gli Utenti (senza distinzione Compagnie Associate/non associate)
- Sarà utilizzabile esclusivamente in fase liquidativa, fino a quando il quadro normativo non ne consentirà l'uso in fase assuntiva. In ogni caso, se interverrà la normativa che consentirà l'eventuale utilizzo del Portale anche in fase assuntiva, lo stesso sarà preliminarmente sottoposto all'Autorità
- Sarà alimentato dai flussi provenienti dalle Compagnie aderenti al Progetto, che immetteranno i dati dei sinistri (*slide 21 + All. 1*)
- Elaborerà i dati inseriti con l'obiettivo di pervenire alla determinazione degli indici di anomalia per ciascun sinistro (*slides 22-24*)
- Sarà consultabile esclusivamente dagli Utenti abilitati (*slides 25-27*)
- Non sarà consultabile dalle Compagnie in modalità massiva ma solo con riferimento ad uno specifico Codice sinistro per il quale si intende svolgere approfondimenti antifrode. A tal fine sarà previsto uno strumento di reporting dei log degli accessi per monitorare che la tipologia e la numerosità degli accessi siano adeguati/proporzionati alle finalità dello strumento (*slides 25-27*)
- Prevederà delle regole informatiche che guidino verso un utilizzo corretto del Portale da parte delle Compagnie (ad esempio blocchi all'applicazione dopo un numero di accessi al superamento di determinate soglie) (*slides 25-27*)
- Al corretto funzionamento del Portale sovrintenderà un Organismo di Garanzia, cui potranno rivolgersi gli assicurati che lamentino problematiche connesse all'utilizzo del Portale da parte della Compagnia responsabile della gestione del sinistro (*slide 29-30*)

Caratteristiche del Portale: *gli aspetti data protection*

- Il Trattamento avrà come base giuridica il legittimo interesse a fronte di un *Legitimate Interest Assessment*, che ha evidenziato che l'interesse perseguito risponde ai seguenti requisiti:
 - liceità;
 - chiarezza;
 - concretezza ed attualità.
- Il trattamento avverrà nel rispetto del principio di minimizzazione dei dati: impegnandosi ANIA a raccogliere esclusivamente le informazioni essenziali e connesse al sinistro (Allegato 1)
- L'*Assessment* eseguito ha evidenziato la «necessità» del trattamento rispetto alla finalità perseguita con il Portale
- ANIA ha interesse a definire le regole che si applicano al trattamento dei dati eseguito tramite il Portale tramite un Codice di Condotta (ex art. 40 GDPR) da presentare e sottoporre alle associazioni degli interessati maggiormente coinvolte nel Progetto (es. associazioni di consumatori)
- L'informativa sul Portale, che sarà fornita agli interessati dalle Compagnie di assicurazione e attraverso il sito dell'ANIA, sarà preliminarmente condivisa con le associazioni coinvolte in modo da avere delle formulazioni, chiare, sintetiche e complete
- Il Portale fornirà alle compagnie dei segnali di anomalia che saranno oggetto di valutazione degli addetti antifrode di ciascuna compagnia (non vi saranno trattamenti basati su decisioni automatizzate)

Soggetti abilitati all'accesso

Associate ANIA

- Le Compagnie assicurative associate ad ANIA contribuiscono alla realizzazione del Portale versando un contributo straordinario, calcolato secondo logiche di proporzionalità.
- Pertanto, tali Compagnie potranno accedere al Portale senza versare alcun ulteriore contributo

Non Associate ANIA

- Le Compagnie assicurative non associate ad ANIA avranno la possibilità di accedere al Portale **corrispondendo un contributo che sarà quantificato nel rispetto dei principi di parità di trattamento e non discriminazione** rispetto a quanto versato dalle associate.
- I contenuti resi accessibili alle Compagnie non associate saranno **i medesimi visualizzabili dalle associate**

Soggetti Istituzionali

- I soggetti istituzionali (a titolo esemplificativo, IVASS, Procure della Repubblica, Polizia di Stato, Arma dei Carabinieri e Guardia di Finanza) avranno accesso **a titolo gratuito** al Portale
- A tali soggetti sarà garantito accesso integrale a **tutte le informazioni contenute nel Portale**.

Regolamento del Portale: elementi essenziali

- La **finalità** per cui è consentito l'accesso alla banca dati, ossia la verifica dell'anomalia (potenziale rischio frode) del singolo sinistro, al fine di poter procedere alle ulteriori indagini antifrode.
- L'**elenco dei soggetti abilitati** a consultare la banca dati
- Le **tempistiche massime** per il conferimento dei dati da parte della Compagnia
- L'**elenco degli obblighi** cui sono soggetti gli utenti che comprenderanno, in via esemplificativa: i) rispettare tutte le disposizioni delle Condizioni di Servizio di volta in volta in vigore; ii) dotarsi, a proprie spese, dell'hardware necessario, di infrastruttura di rete e software per accedere al Portale; iii) fornire informazioni complete sui soggetti autorizzati ad accedere al Portale ed ogni aggiornamento dei soggetti abilitati; iv) porre in essere tutte le attività necessarie per prevenire e/o eliminare eventuali operazioni fraudolente, adottando la massima diligenza; v) non cedere a terzi, a titolo gratuito od oneroso, le informazioni acquisite tramite il Portale.
- I **controlli** che ANIA eseguirà sull'utilizzo del Portale e le relative sanzioni. In particolare, sarà stabilito che ANIA - nell'esercizio dell'attività di gestione e verifica degli utilizzi del Portale - potrà: i) richiedere agli Utenti le informazioni ritenute necessarie in relazione a particolari accessi, ritenuti anomali, al Portale; ii) sospendere temporaneamente l'utilizzo di una credenziale di accesso al Portale, ove abbia riscontrato un'anomalia nell'operatività di tale utenza; iii) disabilitare definitivamente l'utenza dell'impresa, informandone l'impresa, qualora si verificassero ripetute anomalie negli accessi, ovvero il mancato rispetto delle disposizioni normative vigenti o del Regolamento.
- Le **sanzioni** da irrogare in caso di ripetute e comprovate violazioni delle prescrizioni del Regolamento.

Codice di Condotta: elementi essenziali rilevanti ai sensi della normativa privacy

- Il Codice di Condotta individua e fissa delle regole, condivide con associazioni e organismi rappresentativi delle diverse categorie di interessati coinvolti per la gestione delle informazioni che confluiscono nel Portale Antifrode.
- Elementi principali:
 - Assenza di dati giudiziari ex art. 10 GDPR
 - Assenza di dati particolari salvo che indicazione di un valore aggregato
 - Utilizzo del Portale da parte delle compagnie per la valutazione del rischio frode rispetto al sinistro conferito, al fine di poter procedere alle ulteriori indagini antifrode in fase liquidativa
 - Individuazione di set di informazioni necessarie alla definizione del sinistro e alla valutazione del rischio frode
 - Individuazione delle modalità per rendere le informazioni ex art. 13 e 14 GDPR alle categorie di interessati coinvolte
 - Definizione del contenuto delle informazioni da rendere con le associazioni di categorie interessate
 - Modalità di esercizio dei diritti degli interessati
 - Definizione di stringenti misure di sicurezza
 - Devoluzione all'Organismo di Garanzia dei compiti di vigilanza sul rispetto del Codice di Condotta da parte degli aderenti

Dettaglio delle modalità di funzionamento del Portale

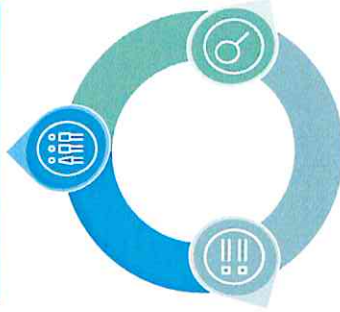
L'input: conferimento dei dati di sinistro

E' stata definita una lista di dati richiesti alle Compagnie per alimentare la Banca Dati, attualmente al vaglio anche dell'Autorità Garante per la Protezione dei Dati Personali

Tipologia dei dati conferiti

- Codice Fiscale /P, IVA;
- Nominativo persona;
- Denominazione società;
- CAP residenza del Contraente;
- Ordine di appartenenza;
- ...

Le anagrafiche dei soggetti coinvolti



Caratteristiche del sinistro

- Ramo ministeriale;
- Garanzia colpita;
- Decorrenza e scadenza garanzia;
- Luogo di accadimento sinistro;
- Data di accadimento del sinistro;
- ...

Ulteriori dettagli per specifiche garanzie

- Malattia e Infortuni
- Strutture sanitarie coinvolte;
- Incendio e Altri Danni ai Beni
- Dati Catastali e immobiliari;
- ...

- I sinistri conferiti dalle Compagnie al momento dell'apertura verranno conservati per i **5 anni successivi alla chiusura** della pratica;

- Per consentire il corretto avvio dell'operatività del Portale, verrà chiesto alle Compagnie di contribuire – **una tantum in fase di set up della banca dati** – i sinistri degli ultimi 5 anni.

Lista di dettaglio dei dati conferiti in Allegato 1

Modalità di determinazione degli indici di anomalia

Per ciascun sinistro conferito, Il Portale elabora due indicatori di anomalia basati rispettivamente su regole esperte (Expert Index) e su analisi statistiche (Anomaly Index), compendiate in un indice sintetico che ne rappresenta la media ponderata (Risk Index)

- Il Portale calcola gli indicatori di anomalia associati a ciascuna regola esperta (quindi deterministica) predefinita per la tipologia di sinistro in esame e li riassume nell'indicatore sintetico **Expert Index** (con valori da 1 a 100). La scelta delle regole esperte da utilizzare nella composizione dell'indice e l'assegnazione dei relativi pesi sarà personalizzabile da parte di ciascuna compagnia (v. *Tavola 1*);

- Il Portale applica un algoritmo di **Anomaly Detection** che, sulla base di una analisi statistica multidimensionale su tutte le variabili disponibili, valuta la distanza tra il sinistro e la configurazione tipica dei sinistri della stessa tipologia. Il risultato dell'algoritmo è rappresentato dall'indicatore **Anomaly Index** (con valori da 1 a 100), corredato dai principali elementi che spiegano la distanza del sinistro dalla norma (v. *Tavola 2*);

- Il Portale genera l'indicatore sintetico **Risk Index** (con valori da 1 a 100), che rappresenta il livello di anomalia complessivo rilevato per il sinistro, sulla base di una media ponderata di **Expert Index** e **Anomaly Index**. La ponderazione, predefinita al 50%, potrà essere modificata autonomamente da ciascuna Compagnia, producendo quindi un **Risk Index** del tutto personalizzato.



Expert index: criteri per l'identificazione e gestione delle regole esperte

ANIA propone la metodologia sotto descritta per la definizione di un primo set di regole esperte e dei relativi pesi, personalizzabili da parte di ciascuna compagnia

Tavola 1

1 Verranno individuati e confermati gli ambiti logici dedotti dalla consolidata esperienza della Banca Dati AIA (*), che ha dimostrato una comprovata utilità nell'indirizzare l'attività antifrode delle imprese. Sulla base di tali criteri sarà elaborata una prima lista di regole esperte;

2 Attraverso il confronto con gli esperti antifrode delle Compagnie, si provvederà all'eventuale integrazione della lista e si formulerà una prima ipotesi di rilevanza relativa di ciascuna categoria di regole (il «peso»);

3 In ogni caso, sarà facoltà di ogni Compagnia scegliere autonomamente dalla lista le regole di interesse e di attribuirvi un peso diverso rispetto a quello pre-identificato secondo la procedura sopra descritta.

(*) Provv. IVASS n.47 del 1/6/2016

Ambito logico della regola	Razionale	Esempio da AIA
Ripetività sul soggetto/bene assicurato	La recidiva di sinistri da parte dello stesso soggetto/bene assicurato (es. targa), eventualmente con più compagnie, può essere indicatore di comportamenti fraudolenti	VEI1: N sinistro/i accaduti in Y mesi
Accadimento rispetto al periodo di copertura	L'accadimento del sinistro immediatamente dopo l'avvio della copertura può nascondere l'esistenza di danni pregressi non coperti, mentre l'accadimento a ridosso della scadenza può nascondere fenomeni speculativi	CON1: N sinistro/i in Y anni nei X giorni successivi alla decorrenza o antecedenti alla scadenza della polizza
Tardività della denuncia	La denuncia tardiva rappresenta un comportamento anomalo per lo più ingiustificato e rende problematico l'accertamento del danno e delle circostanze, prestandosi così a coprire fenomeni fraudolenti	VEI4: N denunce tardive per danni al veicolo in Y anni
Ricorrenza altri soggetti/entità	La ricorrenza su più sinistri di soggetti/entità in determinati ruoli (come ad esempio il testimone), può essere indizio della non genuinità delle dinamiche di sinistro rappresentate	SCO6: testimone presente in più di N sinistri in Y anni
Effettiva abilitazione dei professionisti coinvolti	La presenza di professionisti (es: legali) non iscritti all'albo può essere indizio di intenti speculativi/fraudolenti	SINI1: perito non iscritto/cancellato all'albo
Compatibilità del danno con situazioni pregresse	La presenza di danni pregressi della medesima tipologia può nascondere l'intento di ottenere un risarcimento multiplo per la stessa fattispecie	SCO8: danneggiato/i con lesione pregressa presente in BDS in Y anni
Caratteristiche del bene assicurato	La mancanza di rispondenza del bene assicurato a determinati criteri di conformità può essere indizio di comportamenti speculativi	VEI10: veicolo/i distrutto/i o radiato/i o demolito/i
Legami tra soggetti	La presenza in più sinistri di combinazioni di soggetti/entità (es: legale, centro di cura, testimone) può essere indizio di attività organizzate ad alterare la genuinità dei sinistri	la gestione network presso AIA è attualmente in fase di sviluppo

Anomaly Index: Algoritmo e indicatori di Anomaly Detection

Tavola 2

- Stante l'**indisponibilità della variabile risposta** in Banca Dati (frode conclamata sul sinistro), non può essere adottato un algoritmo statistico di tipo strettamente predittivo, che possa essere addestrato in fase di set-up e apprendere automaticamente sulla base di feedback sul correttezza delle sue indicazioni;
- In questo contesto, l'algoritmo individuato appartiene alla famiglia dell'**anomaly detection** - di tipo *unsupervised* - e genera un Anomaly Index che non può essere considerato strettamente predittivo del rischio frode;
- In particolare, l'algoritmo, sulla base di una **analisi statistica multidimensionale** sulle variabili disponibili in banca dati, valuta la distanza tra il sinistro e la configurazione tipica dei sinistri della stessa tipologia, cioè con la «norma» intesa in senso statistico. Lo **scostamento dalla norma** non implica necessariamente frodolenza, ma può costituire un segnale di attenzione per l'esperto antifrode di Compagnia;
- Per rappresentare il **funzionamento dell'algoritmo** è possibile immaginare ogni sinistro come posizionato in uno spazio multidimensionale del quale le variabili presenti in Banca Dati costituiscono le dimensioni. Sulla base di metriche per il calcolo della distanza tra vettori numerici (es. distanza di Mahalanobis), si procede quindi a calcolare la «lontananza» tra un determinato sinistro e gli altri presenti in Banca Dati. Intuitivamente, un sinistro con una **distanza elevata avrà pertanto una combinazione di variabili rara e distintiva**;
- Le variabili su cui viene calcolata la distanza afferiscono ai medesimi ambiti logici considerati per la costruzione delle regole esperte, tuttavia l'**algoritmo** è in grado di **segnalare situazioni anomale senza l'ausilio di soglie e pesi predeterminati** dall'esperienza umana. In questo modo, grazie alla capacità computazionale delle macchine, è quindi possibile intercettare schemi non identificabili mediante regole deterministiche, che sono strutturalmente in grado di considerare un numero limitato di caratteristiche (tipicamente una o al massimo due variabili incrociate per ciascuna regola esperta);
- Il Portale antifrode fornirà l'indicatore sintetico **Anomaly Index corredato dalle prime 5 anomalie statistiche** (laddove significative) in ordine di rilevanza, rappresentate in modalità «human readable».

Misure di sicurezza (1/3)

Dispositivi per la sicurezza dei dati e prevenzione delle 'intrusioni'

- Accesso attraverso **connessioni sicure** (MPLS/VPN) protette da **certificati di crittografia** rilasciati da una certification authority;
- Meccanismi di **autenticazione a due fattori**;
- Meccanismi di controllo (es. OTP, captcha) per **scongiurare eventuali tentativi di accesso con sistemi automatici**;
- Dispositivi per la **verifica** – tramite il Portale - **sulle diverse componenti di sicurezza del sistema** (informatica, legale ed organizzativa) nonché l'accesso ai dati in conformità ai principi della certificazione ISO27001;
- Strumenti idonei a consentire la **verifica dell'implementazione delle procedure di sicurezza** nonché lo svolgimento di **audit** in ambito compliance data protection;
- Regolare esecuzione di **penetration tests**.

Misure di sicurezza (2/3)

Governo e controllo degli accessi

- **Controllo sistematico degli accessi**, in termini di autenticazione e autorizzazione per ogni tipo di interfaccia di collegamento (accessi Application to Application – A2A – e accesso manuale al front-end);
- **Profili di utenza differenziati** secondo un approccio cosiddetto **RBAC – Role-Based Access Control**, che disciplina le regole di visibilità ed i privilegi dell'utente in funzione del ruolo dello stesso e dell'organizzazione di appartenenza;
- Accessi per le Compagnie in ogni caso sempre limitati all'investigazione di uno **specifico sinistro conferito**, che non possono essere **in nessun caso di tipo massivo**;
- **Credenziali di autenticazione** rilasciate da ANIA con un processo rigoroso ai soggetti istituzionali nonché ai soggetti identificati dalle singole Compagnie;
- **Log di ogni accesso al sistema** contenente informazioni chiave per il **monitoraggio del comportamento degli utenti** (data, orario, tipo di operazione, utenza, organizzazione, ...). Attraverso i log si potrà:
 - Generare **reportistica di controllo** periodica, in modo da evidenziare trend anomali;
 - Effettuare **verifiche puntuali** per approfondire situazioni particolari;
 - Avviare **procedure organizzative per il controllo costante delle abilitazioni** (es. cancellazione utenze non attive);
 - Attivare **eventuali azioni automatiche di blocco** in funzione di parametri e soglie predefiniti.

Misure di sicurezza (3/3)

Strumenti per la gestione della sicurezza e corretta gestione dei dati

- **Console di Customer Boarding:** console preposta al censimento e alla gestione centralizzata delle strutture organizzative e alla definizione di attributi ed abilitazioni;
- **Dashboard di Profilazione utente:** per configurare la profilazione a livello di singola Compagnia;
- **Sistema di Logging:** ciascun processo e funzione lascia una traccia (“log”) con le informazioni di richiedente, richiesta e risultato;
- **Console di IP Filtering:** strumento che consente il censimento dell’elenco indirizzi IP autorizzati ad accedere al Sistema;
- **Procedure di Storizzazione:** procedure che gestiscono automaticamente la storizzazione/cancellazione dei dati secondo le regole di conservazione definite;

OMISSIS

Organismo di Garanzia (1)

- Sarà costituito da 3 o 5 **soggetti indipendenti dalle Compagnie**, designati dall'ANIA e dalle associazioni maggiormente rappresentative delle categorie/ordini professionali coinvolti. Ciascuno dei componenti dovrà garantire e mantenere requisiti di onorabilità, professionalità, capacità ed indipendenza. La presidenza sarà assegnata ad una personalità di altissimo profilo (ex magistrato, ex dirigente IVASS...)
- Dal punto di vista organizzativo, l'Organismo di Garanzia sarà incardinato all'interno dell'Osservatorio Antifrode dell'ANIA, che svolge attività di sensibilizzazione alla prevenzione del rischio frode in ambito assicurativo e di promozione di modelli di controllo volti a contrastare i fenomeni fraudolenti.
- L'Organismo di Garanzia sarà dotato di una sua **autonomia finanziaria**, con un budget annuo non inferiore a 300.000 euro. Tali risorse saranno utilizzate in piena autonomia per l'esercizio delle proprie funzioni.
- A titolo esemplificativo, L'Organismo di Garanzia potrà:
 - **verificare e monitorare l'osservanza delle regole del Codice di Condotta** da parte delle Compagnie;
 - **verificare e gestire le segnalazioni ed i reclami** eventualmente insorti tra le Compagnie, gli assicurati e gli interessati, relativamente alle violazioni del Regolamento e del Codice di condotta;
 - **attivarsi nei confronti delle Compagnie per richiedere l'adozione degli interventi correttivi** necessari al fine di rimuovere i profili di non conformità al Regolamento e al Codice di Condotta eventualmente riscontrati;
 - **accedere alle informazioni** necessarie per lo svolgimento dei propri compiti, avvalendosi, se necessario, di consulenti esterni, utilizzando a tal fine le risorse finanziarie (budget) ad esso assegnate;
 - in conseguenza dei controlli effettuati a seguito di segnalazioni e/o reclami, **applicare sanzioni alle Compagnie** secondo la gravità della violazione eventualmente riscontrata;

Organismo di Garanzia (2)

- **Piena conoscibilità da parte dei consumatori**, che riceveranno le informazioni sull'esistenza del Portale e dell'Organismo di Garanzia ed il relativo funzionamento sui siti istituzionali dell'ANIA, nonché all'interno dell'informativa rilasciata dalla compagnia assicurativa di riferimento
- **Piena accessibilità**, tramite più canali dedicati (posta elettronica, casella postale, form online)
- **Ampie garanzie procedurali**: tempi prestabiliti per l'esame del reclamo; pienezza del contraddittorio in ogni fase della procedura, tramite la possibilità di depositare memorie e chiedere di essere sentiti
- **Piena trasparenza nei confronti delle Autorità di settore**: annualmente, l'OdG dovrà fornire al Garante Privacy e AGCM un resoconto riassuntivo dei controlli e delle verifiche effettuate, delle procedure di reclamo definite e delle misure sanzionatorie eventualmente adottate.

Allegato 1

Dettaglio dei dati conferiti dalle Compagnie in
relazione al Portale

Dettaglio dei dati conferiti dalle Compagnie (1/3)

La lista di seguito rappresentata costituisce l'elenco dei dati che ANIA ritiene necessari per l'operatività del Portale. Tale elenco potrà subire una riduzione in considerazione delle interlocuzioni ancora in corso con il Garante per la Protezione dei Dati Personali. Eventuali modifiche alla lista dei dati conferiti saranno sottoposte all'attenzione dell'AGCM

Rami	Dati Conferiti
Informazioni generali valide per tutti i rami Danni Non Auto e Vita (Puro rischio) - Anagrafiche dei soggetti coinvolti	<u>Codice Fiscale/ nominativo persona o Partita IVA/ denominazione di società di:</u>
	Assicurato
	Beneficiario
	Contraente
	Legale fiduciario
	Legale di controparte
	Medico legale fiduciario
	Medico di controparte
	Investigatore
	Testimone
	Intermediario
	Danneggiato
	Perito fiduciario
	Perito controparte
	Carrozzeria
	Medico di controparte
	Ordine di appartenenza del Legale fiduciario
	Ordine di appartenenza del Legale di controparte
	Ordine di appartenenza del Medico legale fiduciario
	Ordine di appartenenza del Medico di controparte
CAP residenza del Contraente	
Targa del veicolo e/o altro mezzo (se garanzia CVT)	

Dettaglio dei dati conferiti dalle Compagnie (2/3)

Rami	Dati Conferiti
<p>Informazioni generali valide per tutti i rami Danni Non Auto e Vita (Puro rischio) - Caratteristiche del sinistro</p>	Ramo ministeriale
	Numero del sinistro
	Partita di danno
	Tipologia garanzia relativa al sinistro
	Data di decorrenza garanzia
	Data di scadenza garanzia
	Somma assicurata / Capitale assicurato garanzia
	Area geografica: CAP luogo di accadimento sinistro
	Denominazione impresa che ha in gestione il sinistro
	Data di accadimento del sinistro
	Data denuncia sinistro all'impresa
	Stato sinistro: Aperto non pagato
	Stato sinistro: Pagamento parziale
	Stato sinistro: Pagamento totale
	Stato sinistro: Senza seguito
	Stato sinistro: Riapertura
	Autorità intervenute
	Intervento legale: SI/NO
	Contenzioso in corso: SI/NO

Dettaglio dei dati conferiti dalle Compagnie (3/3)

Rami	Dati Conferiti
<p>Ramo 1 - Infortuni</p>	<p>Morte/ infortunio (solo evento) Macrolesione SI/NO Ospedale di prima refertazione Case di cura private o Centri medici privati e/o riabilitativi che hanno effettuato prestazioni Diaria da gesso: SI/ NO</p>
<p>Ramo 2 - Malattia</p>	<p>Macrolesione SI/NO Ospedale di prima refertazione Case di cura private o Centri medici privati e/o riabilitativi che hanno effettuato prestazioni Diaria giornaliera: SI/ NO</p>
<p>Ramo 8 - Incendio ed elementi naturali Ramo 9 - Altri danni i beni</p>	<p>Dati catastali e dei registri immobiliari Indicazione di un ulteriore contratto assicurativo sul medesimo rischio presso un'altra impresa di assicurazione - rif. art. 1910 c.c.- (SI/ NO e se SI denominazione dell'impresa) Società di salvataggio (interventi di ripristino: SI/ NO)</p>