Euroconference

In collaborazione con:

TeamSystem®

GRUPPO progetto studio

PRIVACY TOUR

Euroconference

In collaborazione con:

TeamSystem®

GRUPPO progetto studio

ADEMPIMENTI PRIVACY ALLA LUCE DEL NUOVO REGOLAMENTO UE N. 679/2016

a cura di Gianluca Mazzoli

IL NUOVO REGOLAMENTO UE SULLA PRIVACY:

CASI D'USO PRATICI

GDPR – Cosa fare per essere compliant?

- Organigramma/Mapping delle risorse chiave in azienda
  - Titolari, Responsabili, DPO, Soggetti Autorizzati
- Registro dei Trattamenti
- Registro dei Consensi
- Data Breach
- Mapping degli Asset aziendali
  - Per ognuno effettuare un'Analisi dei Rischi
- Produzione documenti di nomina, registri trattamenti, informative, etc…
- Audit periodiche (almeno 1 volta all'anno)
- Privacy By Design / By Default
  - Assicurati che il tuo fornitore di software abbia adeguato al GDPR l'applicativo che utilizzi
  - Se pensi di sviluppare un nuovo progetto tieni ben presente i principi di privacy by design e by default

GDPR – Dato personale, cos'è e perché è importante?

COSA?

Qualsiasi dato relativo a individui identificabili

- Dipendenti, fornitori, clienti
- Nomi
- Indirizzi
- Indirizzi email
- Numeri di telefono
- Informazioni c.d. «sensibili»

PERCHE'?

Il GDPR ci chiede

- Come vengono ottenuti
- Perchè sono gestiti
- Come sono gestiti
- Per quanto tempo
- A chi possono essere comunicati

GUIDA PRATICA: 12 cose da fare da subito

1. Consapevolezza
2. Informazioni in tuo possesso
3. Comunicazione delle informative sulla privacy
4. Diritti dell'interessato
5. Richieste di accesso ai dati da parte del soggetto interessato
6. Base giuridica per il trattamento dei dati personali
7. Consenso
8. Minori
9. Data Breach
10. Protezione dei dati mediante valutazione dell'impatto sulla protezione dei dati e sulla progettazione
11. DPO
12. Considerazioni internazionali

(Rif. Guide to GDPR – ICO Information Commissioner's Office)

1

Consapevolezza

- Chi sono le figure chiave in azienda
- Avere coscienza dell'impatto della normativa in azienda
- Conoscere quali e quante risorse possono essere necessarie per adeguarsi
- Avere coscienza dei rischi nei trattamenti aziendali

2

Informazioni in tuo possesso

- Condurre una verifica completa dei dati in tutta l'organizzazione:
  - Documenta quali dati hai (e da dove li hai ottenuti)
  - Documenta con chi stai condividendo i dati

- Sapere quali dati hai, da dove proviene e con chi li condividi ti aiuterà a rispettare il principio di responsabilità del GDPR.

3

Comunicazione delle informative sulla privacy

- Rivedi la tua attuale politica sulla privacy / informativa sulla privacy
- Informativa sulla privacy per far sapere alle persone chi sei e come intendi utilizzare i loro dati

- Devi spiegare:
  - La tua base legale per l'elaborazione dei dati
  - Periodi di conservazione
  - Che le persone possono rivolgersi ad un Responsabile per qualunque problema

- **Tutto ciò deve essere fatto con un forma concisa e trasparente, con linguaggio semplice, facile da capire e chiaro!**

4

Diritti dell'interessato

- Diritti per gli individui:
  - Per modificare i propri dati
  - Per cancellare le informazioni
  - Per prevenire il marketing diretto
  - Per evitare processi decisionali automatizzati e di profilazione
  - Portabilità dei dati

5

Richieste di accesso ai dati da parte del soggetto interessato

- Le regole per queste richieste cambieranno con il GDPR
- Nessuna multa nella maggior parte dei casi
- Avresti solo 15 giorni per conformarti
- È inoltre necessario disporre di politiche / procedure per rifiutare le richieste
- È necessario fornire politiche di conservazione e politiche di correzione

- **Considera di condurre un'analisi costi / benefici per munirti di uno strumento cloud che ti consenta di gestire questo scenario.**

6

Base giuridica per il trattamento dei dati personali

- Rivedi e documenta la base legale per l'elaborazione dei dati
- Le basi legali devono essere spiegate nella tua informativa sulla privacy
- Le basi legali devono essere spiegate nelle richieste di accesso

- **Documentalo perché aiuta a soddisfare i requisiti di responsabilità del GDPR**

7

Consenso

- Assicurati che i tuoi consensi soddisfino gli standard del GDPR
- Il consenso deve essere verificabile e gli interessati hanno generalmente diritti più forti quando il consenso è affidato all'elaborazione
- Se il consenso fornito dagli utenti non era chiaro (ad es. se accettavano semplicemente termini e condizioni), dovresti ottenere nuovamente il consenso. Quindi, prepara una funzionalità per inviare email di massa ai tuoi utenti per chiedere loro di andare alla pagina del loro profilo e controllare tutte le caselle di controllo per le attività di elaborazione dei dati personali che hai.
- **CHI TRATTA DATI PERSONALI DEVE POTER DIMOSTRARE CHE IL CONSENSO È STATO FORNITO SE ERA DOVUTO !**
- Assicurati di avere uno strumento di controllo

8

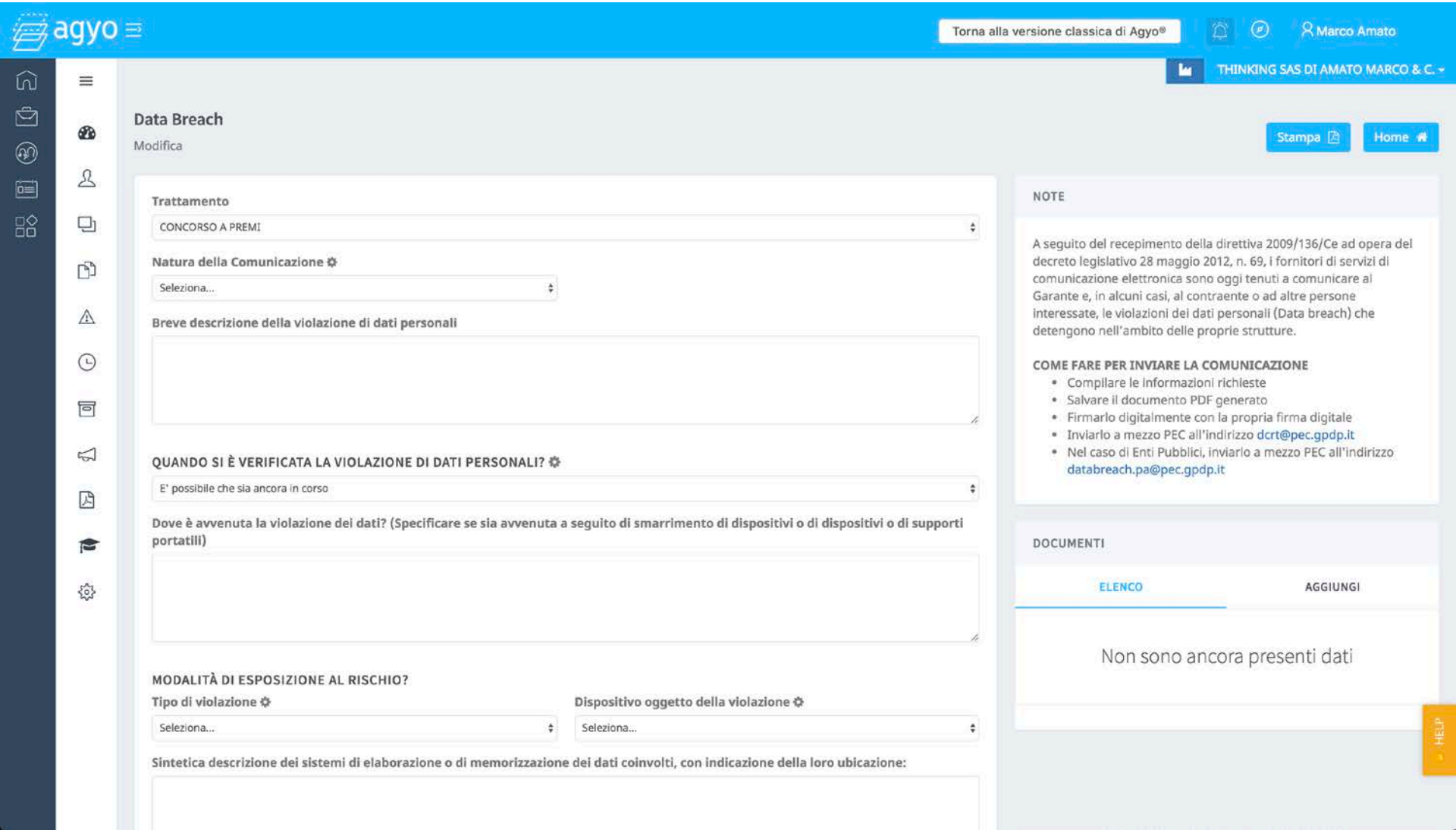
Minori

- Protezione speciale per i dati personali dei minori
- Meccanismo di verifica dell'età
- Consenso dei genitori / tutori
- Ricorda che il consenso deve essere verificabile e che quando si raccolgono dati sui minori la tua informativa sulla privacy deve essere scritta con un linguaggio che anche i minori possano comprendere.

Data Breach

- Dotati di uno strumento per la gestione delle segnalazioni
- Procedure per la risposta e la segnalazione
- Si noti che la mancata segnalazione di una violazione quando richiesto a tal fine potrebbe comportare una multa, nonché una multa per la violazione stessa.

Esempio di Data Breach

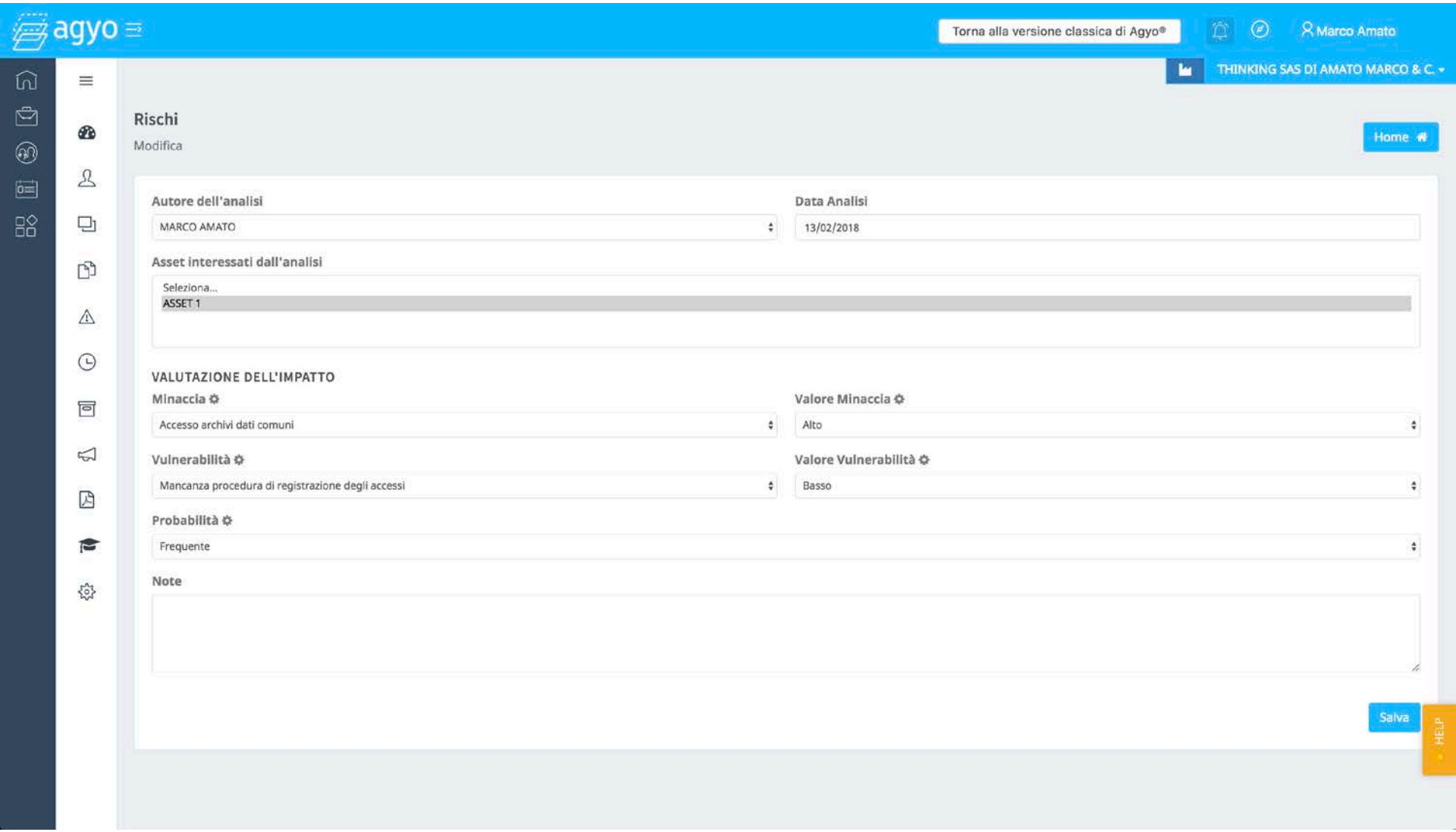


10

Protezione dei dati mediante valutazione dell'impatto sulla protezione dei dati e sulla progettazione

- Familiarizzare con le valutazioni dell'impatto sulla privacy (PIA) e su come implementarle nella tua organizzazione
- Valutare quando sarà necessaria una PIA
- Adottare i principi di privacy by design
- Si noti che non è sempre necessario eseguire una PIA - è richiesta una PIA in situazioni ad alto rischio, ad esempio dove viene impiegata una nuova tecnologia o dove è probabile che un'operazione di profilazione influenzi significativamente le persone.

Esempio

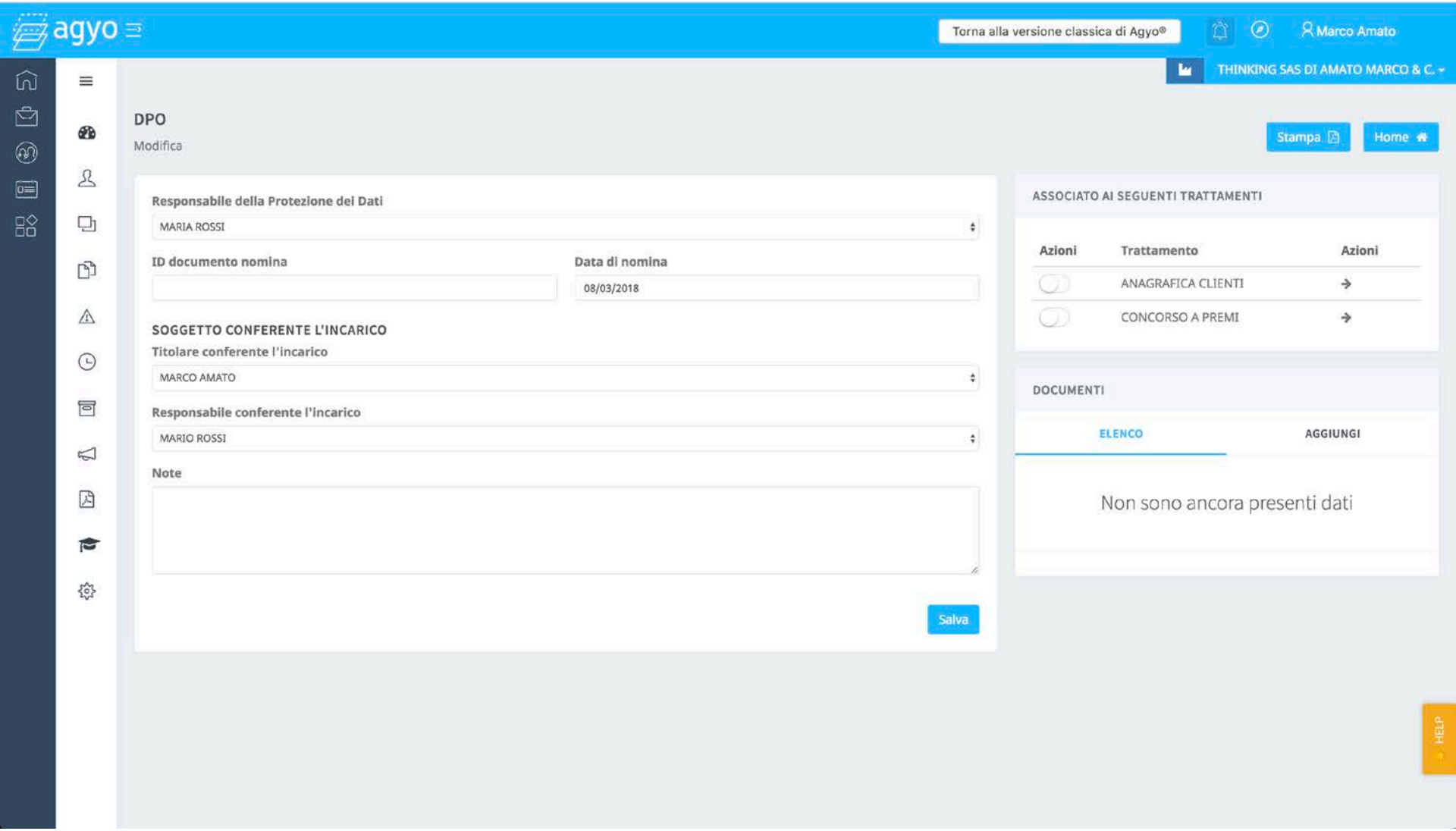

agyo
Torna alla versione classica di Agyo®
Marco Amato
THINKING SAS DI AMATO MARCO & C.
Rischi
Modifica
Home
Autore dell'analisi
MARCO AMATO
Data Analisi
13/02/2018
Asset interessati dall'analisi
Seleziona...
ASSET 1
VALUTAZIONE DELL'IMPATTO
Minaccia
Accesso archivi dati comuni
Valore Minaccia
Alto
Vulnerabilità
Mancanza procedura di registrazione degli accessi
Valore Vulnerabilità
Basso
Probabilità
Frequente
Note
Salva
HELP

DPO

- Solo alcune organizzazioni saranno tenute a nominare un responsabile della protezione dei dati

- Un responsabile della protezione dei dati deve sapere "tutto sulla protezione dei dati" e un'attenta considerazione deve essere fatta quando si tratta della loro posizione all'interno di un'organizzazione.

Esempio


agyo
Torna alla versione classica di Agyo®
Marco Amato
THINKING SAS DI AMATO MARCO & C.
DPO
Modifica
Stampa
Home
Responsabile della Protezione dei Dati
MARIA ROSSI
ID documento nomina
Data di nomina
08/03/2018
SOGGETTO CONFERENTE L'INCARICO
Titolare conferente l'incarico
MARCO AMATO
Responsabile conferente l'incarico
MARIO ROSSI
Note
Salva
ASSOCIATO AI SEGUENTI TRATTAMENTI
Azioni
Trattamento
Azioni
ANAGRAFICA CLIENTI
CONCORSO A PREMI
DOCUMENTI
ELENCO
AGGIUNGI
Non sono ancora presenti dati
HELP

Considerazioni internazionali

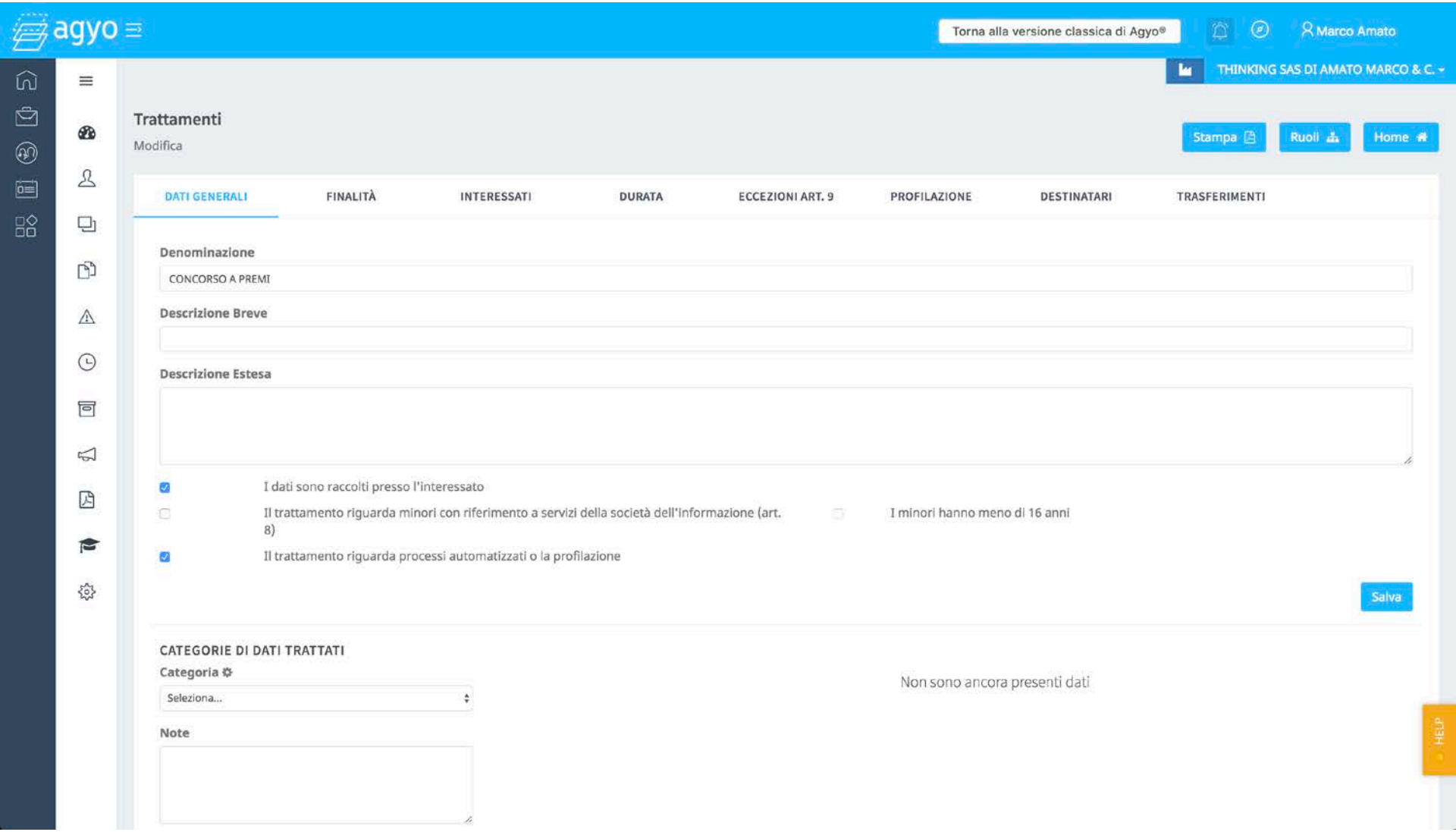
- Disposizioni complesse per stabilire quale autorità di controllo della protezione dei dati assume la guida
- In parole povere, l'autorità capofila viene determinata in base a dove l'organizzazione ha la sua amministrazione principale o dove vengono prese le decisioni sull'elaborazione dei dati.

Registro dei Trattamenti…NO EXCEL!

L'articolo 30 dice che devi tenere un registro di tutti i tipi di attività per le quali usi i dati personali. Sembra burocrazia, ma potrebbe essere utile: potrai collegare alcuni aspetti della tua domanda a quel registro (ad esempio le caselle di controllo del consenso o i record del tuo audit trail).

- E’ importante che il Registro dei Trattamenti sia conservato a norma
- Devi tenere sott’occhio le scadenze dei trattamenti, ed un software potrebbe aiutarti a ricordarle
- Dovrai mappare i dati personali trattati e produrre la relativa documentazione

Esempio


agyo
Torna alla versione classica di Agyo®
Marco Amato
THINKING SAS DI AMATO MARCO & C.
Trattamenti
Modifica
Stampa
Ruoli
Home
DATI GENERALI
FINALITÀ
INTERESSATI
DURATA
ECCEZIONI ART. 9
PROFILAZIONE
DESTINATARI
TRASFERIMENTI
Denominazione
CONCORSO A PREMI
Descrizione Breve
Descrizione Estesa
I dati sono raccolti presso l'interessato
Il trattamento riguarda minori con riferimento a servizi della società dell'informazione (art. 8)
I minori hanno meno di 16 anni
Il trattamento riguarda processi automatizzati o la profilazione
Salva
CATEGORIE DI DATI TRATTATI
Categoria
Seleziona...
Non sono ancora presenti dati
Note
HELP

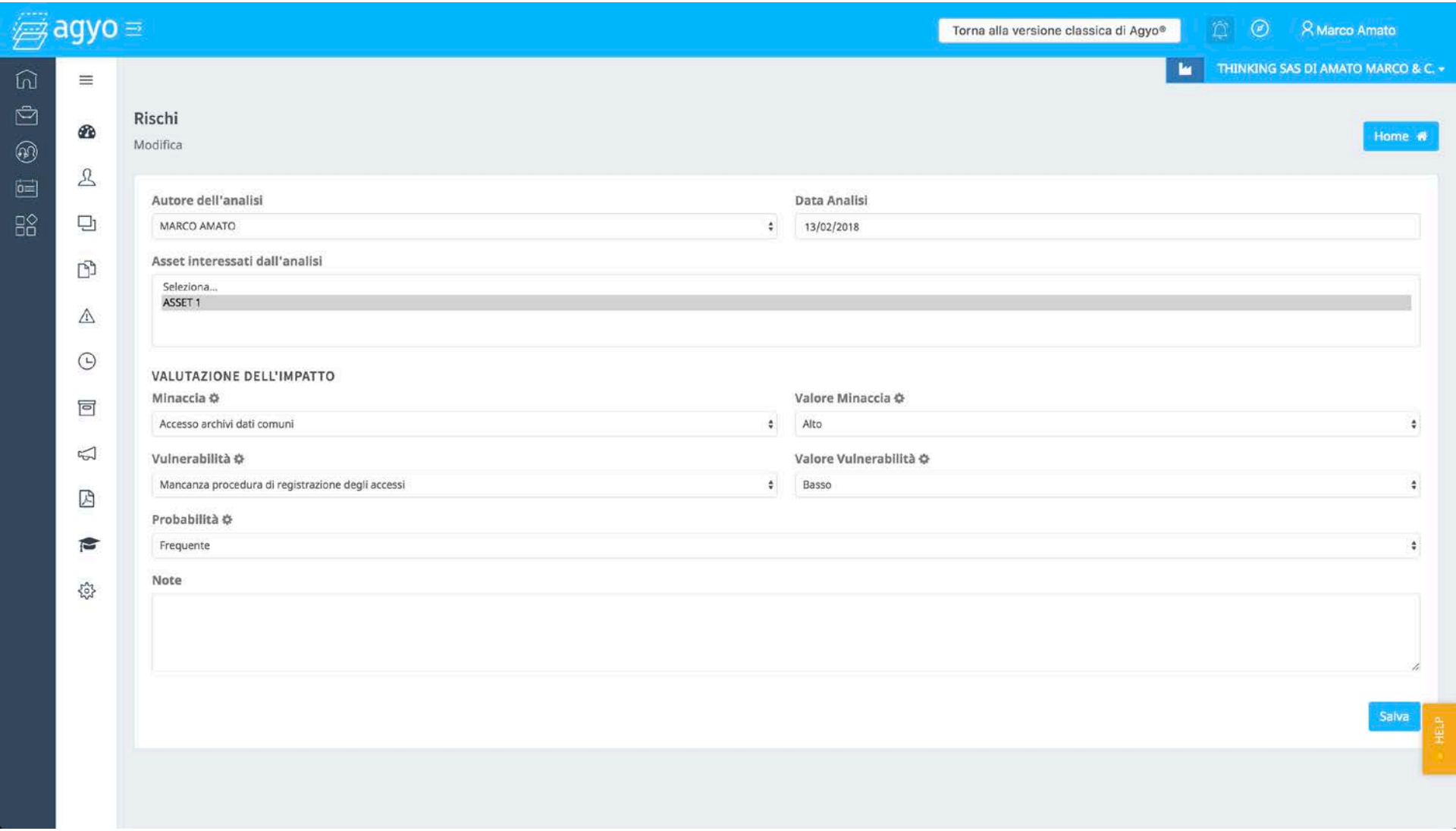
Rischi sulla Protezione dei Dati Personali

- **Violazioni di riservatezza** ad es. informazioni fornite in modo inappropriato, perse o supervisionate

- **Danno alla reputazione**, ad es. il vostro Studio o la vostra Azienda potrebbe subire un danno di immagine se coinvolto in un evento di violazione di dati personali.

- **I Clienti** devono aspettarsi che ci prendiamo cura dei loro dati in modo sicuro e professionale, indipendentemente da eventuali regolamenti!

Esempio


agyo
Torna alla versione classica di Agyo®
Marco Amato
THINKING SAS DI AMATO MARCO & C.
Rischi
Modifica
Home
Autore dell'analisi
MARCO AMATO
Data Analisi
13/02/2018
Asset interessati dall'analisi
Seleziona...
ASSET 1
VALUTAZIONE DELL'IMPATTO
Minaccia
Accesso archivi dati comuni
Valore Minaccia
Alto
Vulnerabilità
Mancanza procedura di registrazione degli accessi
Valore Vulnerabilità
Basso
Probabilità
Frequente
Note
Salva
HELP

Regole per il salvataggio dei dati su carta…

- Conservare i dati in modo sicuro dove le persone non autorizzate non possono accedervi, pensa alla tua famiglia, amici, addetti alle pulizie e appaltatori.
- Sotto chiave e lucchetto quando non in uso
- Rimuovi tutti i documenti con i dati personali immediatamente dalle aree comuni come le stampanti
- Smaltire in modo sicuro
- **Carica tutti i file client su un Cloud certificato o su un applicativo dedicato (CCT) e smaltisci i file cartacei in modo sicuro al completamento della transazione. Non c'è motivo di tenere la carta, è un rischio**

... o in formato elettronico

- Tutti i dati personali devono essere protetti da accessi non autorizzati, cancellazioni accidentali e tentativi di hacking illecito
- Tutti i dati personali devono essere conservati all'interno dell'UE

Dove salvare i dati in formato elettronico?

- Cloud Storage / CCT
  - Funzione di archiviazione per file / documenti elettronici
  - Scansione del telefono, backup, sicurezza
  - Memorizza TUTTI i file su un Cloud certificato o un applicativo dedicato (es: CCT) e cancella tutte le altre copie cartacee ed elettroniche al completamento della transazione.
  - Non archiviare i dati personali del cliente sul tuo PC / laptop hard disk, palmari e dispositivi mobili, dispositivi di archiviazione esterni.
  - Rimuovi tutti i dati del cliente dal tuo PC / laptop, da qualsiasi altro dispositivo di archiviazione esterno e da posizioni di archiviazione cloud non conformi

Regole per l’utilizzo dei dati

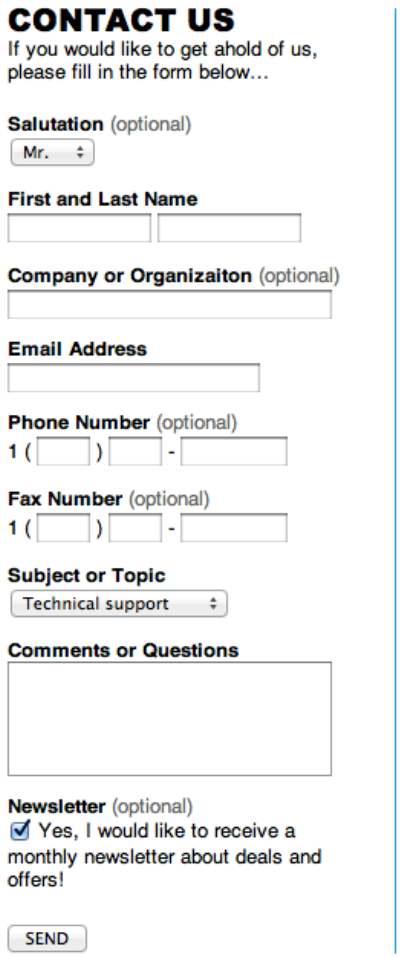
- Blocca lo schermo del tuo pc quando non lo presidi
- Non condividere dati personali in modo informale
- Utilizzare Client di messaggistica sicuri
- Criptare le email
- Non trasferire dati al di fuori dell'UE
- Accedi solo ai dati tramite reti WiFi sicure

Regole per l’accuratezza dei dati

- La legge richiede che il tuo Studio o la tua Azienda e i consulenti garantiscano che i dati siano aggiornati e accurati cosi da:
  - Minimizzare le posizioni di archiviazione. I dati del cliente devono essere conservati in uno Storage Cloud certificato solo in base alle Regole di archiviazione dei dati
  - Aggiorna i dati in ogni occasione e correggi le inesattezze
  - Fornisci ai clienti l'accesso per aggiornare le loro informazioni
  - Tutti i dati di marketing devono essere conformi. I consulenti, per completare la sezione sul consenso al marketing, devono assicurarsi che venga registrato il consenso prestato dai clienti per poter ricevere comunicazioni di marketing dal vostro Studio/Azienda

Non creare Form con campi di cui non hai bisogno

- Si è sempre tentati di inserire campi per raccogliere maggiori info possibili, ma a meno che non si abbia assolutamente bisogno dei dati per fornire il proprio servizio, non si devono raccogliere.
- A meno che tu non stia consegnando qualcosa, l'indirizzo di casa o il telefono non sono necessari.



Non dare per scontato che i tuoi fornitori siano compliant

- Il vostro Studio o la Vostra Azienda sono responsabili in caso di violazione dei dati ad una parte terza (c.d. "processori") a cui si inviano dati personali.
- Quindi, prima di inviare i dati a un altro servizio, assicurati che abbiano almeno un livello base di protezione dei dati.

Non pensare che avere una ISO ti rende compliant

- Le ISO sono un buon inizio e probabilmente sono il 70% di quanto richiesto dalla normativa, ma non sono sufficienti - la maggior parte delle cose sopra elencate non sono contemplate in nessuno di questi standard

Nuovi requisiti informatici

- Oltre ai cambiamenti nelle pratiche per l'archiviazione dei dati, l'uso e la registrazione accurata, assicurarsi quanto segue:
  - Tutti gli hard disk per PC e laptop sono criptati
  - Elimina le vecchie email con dati personali non crittografati
  - Imposta password complesse
  - Non utilizzare dispositivi di archiviazione personali (chiavette USB, dischi rigidi esterni)
  - Email e uso di Internet - Approccio basato sul buon senso
  - Wifi: nuove reti dedicate negli uffici del vostro Studio o della vostra Azienda solo per gli ospiti

Euroconference

In collaborazione con:

TeamSystem®

GRUPPO progetto studio

PRIVACY TOUR

Presentazione della soluzione AGYO PRIVACY - TEAMSYSTEM

a cura di Marco Amato

AGYO PRIVACY

GDPR senza pensieri?
Scegli il software in cloud Agyo Privacy

GRUPPO progetto studio

TeamSystem®

agyo

PRIVACY

Agyo Privacy la soluzione in Cloud per adeguarsi al GDPR

MULTI-AZIENDA
Che tu possieda più società o che tu sia un consulente che gestisce più di un'azienda, Agyo Privacy ti consente di gestirle tutte con lo stesso account.

MULTI-ACCOUNT
Per far sì che il tuo team possa lavorare simultaneamente al processo di compliance.

ACCOUNTABILITY
Gestisci l'organigramma identificando i titolari del trattamento, i responsabili, i soggetti autorizzati e i DPO.

REGISTRO DEI TRATTAMENTI
Attraverso un'interfaccia formata da più step, Agyo Privacy ti guida nella corretta compilazione del Trattamento.

ANALISI DEI RISCHI
Definisci gli assets aziendali, identifica i rischi e applica le misure di sicurezza necessarie: Agyo Privacy ha già catalogato per te tutte le possibili opzioni.

REGISTRO DEI CONSENSI
Tieni traccia di tutte le attività relative ai dati trattati. Inoltre, un set di API ti consentirà di estendere il registro anche ad App e Software sviluppati da terze parti.

agyo

PRIVACY

A CHI SI RIVOLGE?

AZIENDE
Di qualunque dimensione

STUDI PROFESSIONALI
Di qualsiasi tipologia
- Per adeguare la propria organizzazione
- Per offrire consulenza ai propri clienti

CONSULENTI PRIVACY
Per offrire consulenza

ASSOCIAZIONI ED ENTI NON PROFIT
Di qualsiasi tipologia

ENTI E PUBBLICHE AMMINISTRAZIONI
Di qualsiasi tipologia e dimensione

IN GENERALE…
…tutti i soggetti che trattano dati personali e devono adeguarsi al GDPR

agyo

PRIVACY

I BENEFICI DELLA SOLUZIONE

TUTTI I VANTAGGI DEL CLOUD
Nessuna installazione, soluzione sempre disponibile e accessibile h24.

PERCORSO GUIDATO PASSO PASSO
Sei accompagnato in tutte le attività da un percorso che ti evita dimenticanze ed errori

A MISURA DELLE PROPRIE ESIGENZE
Scegli il pacchetto di offerta più adatto alle tue necessità per numero di aziende e trattamenti di dati personali gestiti.

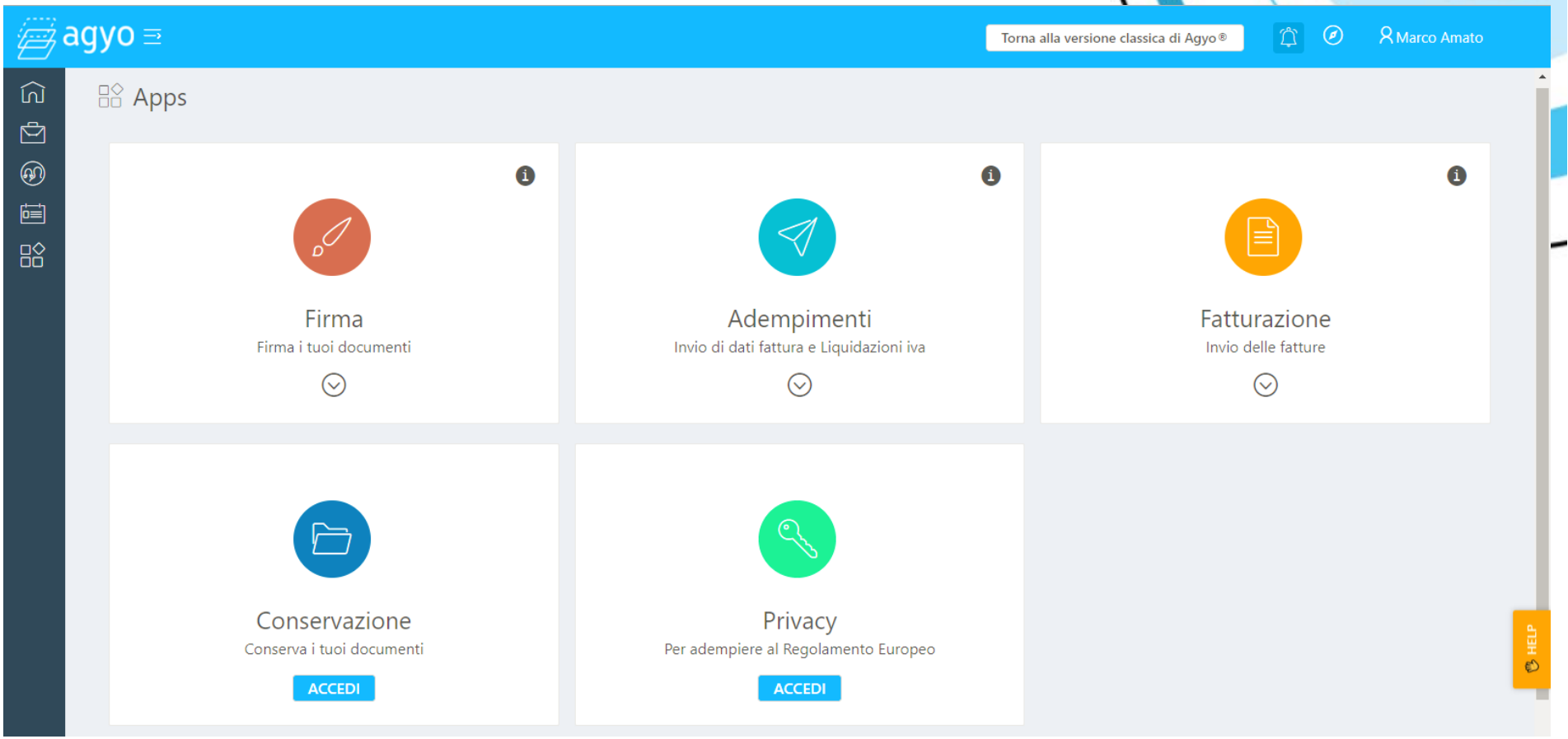
ATTIVITÀ DI CONSULENZA
La soluzione è Multi-Azienda e ti consente di gestire la privacy anche per conto dei tuoi clienti.

TROVA NUOVI CLIENTI
Puoi essere visibile agli altri utenti della piattaforma che possono contattarti grazie alla funzione «Cerca consulente Privacy.

INTEGRATA CON GLI ALTRI SERVIZI TS
Poi beneficiare degli altri servizi di Agyo: firma digitale e conservazione sostitutiva in cloud.
E' integrata anche con i gestionali TeamSystem

agyo

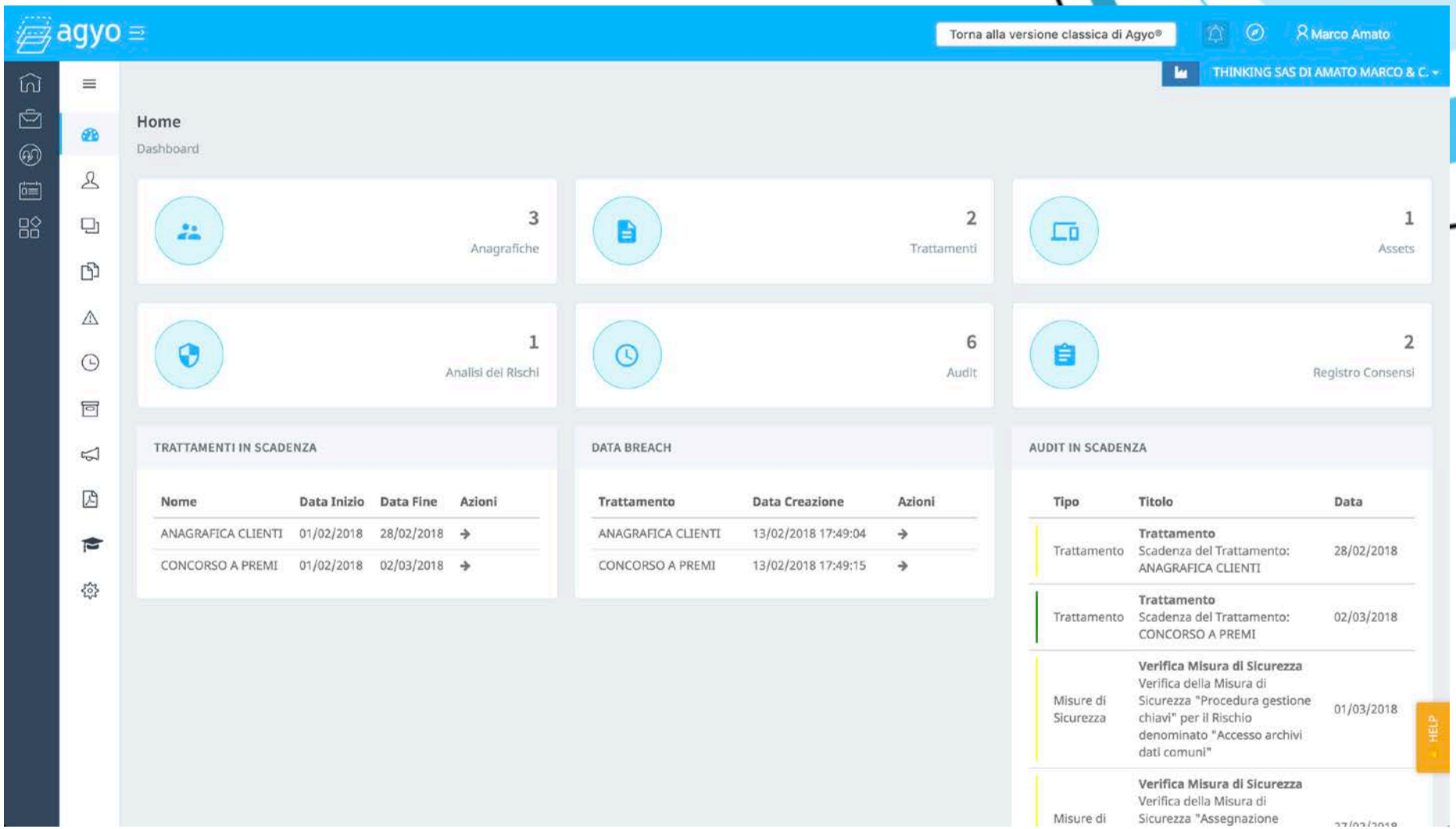
PRIVACY



agyo
PRIVACY

LA DASHBOARD

Per avere sempre tutto sotto controllo



agyo PRIVACY

IL FLUSSO OPERATIVO

Guida passo passo in tutte le attività

AZIENDE
In base al tuo piano, puoi creare e gestire le Aziende per le quali effettuare il trattamento dei dati.

ANAGRAFICHE
Organizza e identifica le risorse della tua azienda che saranno coinvolte nei trattamenti che andrai ad effettuare.

REGISTRO DEI TRATTAMENTI
Tramite una comoda suddivisione a step, è possibile redigere il trattamento in maniera molto semplice ed intuitiva.

TITOLARI
Organizza e identifica i Titolari del trattamento per la tua Azienda.

RESPONSABILI
Organizza e identifica i Responsabili ed i Sub-Responsabili del trattamento per la tua Azienda.

DPO
Organizza e identifica i Responsabili per la Protezione dei Dati (DPO) del trattamento per la tua Azienda.

SOGGETTI AUTORIZZATI
Organizza e identifica i Soggetti Autorizzati del trattamento per la tua Azienda.

ASSET
Organizza e identifica gli Asset per la tua Azienda. Per ognuno di essi potrai effettuare un'Analisi dei Rischi ed implementare le Misure di Sicurezza.

ANALISI DEI RISCHI
Per ogni Asset precedentemente creato per la tua Azienda, puoi effettuare un'Analisi dei Rischi.

MISURE DI SICUREZZA
Per ogni Analisi del Rischio precedentemente creata per la tua Azienda, puoi gestire le Misure di Sicurezza da dover implementare nella tua Azienda.

AUDIT
Tieni sott'occhio tutte le scadenze dei relativi Trattamenti, Revoche degli Incarichi, Misure di Sicurezza, etc...

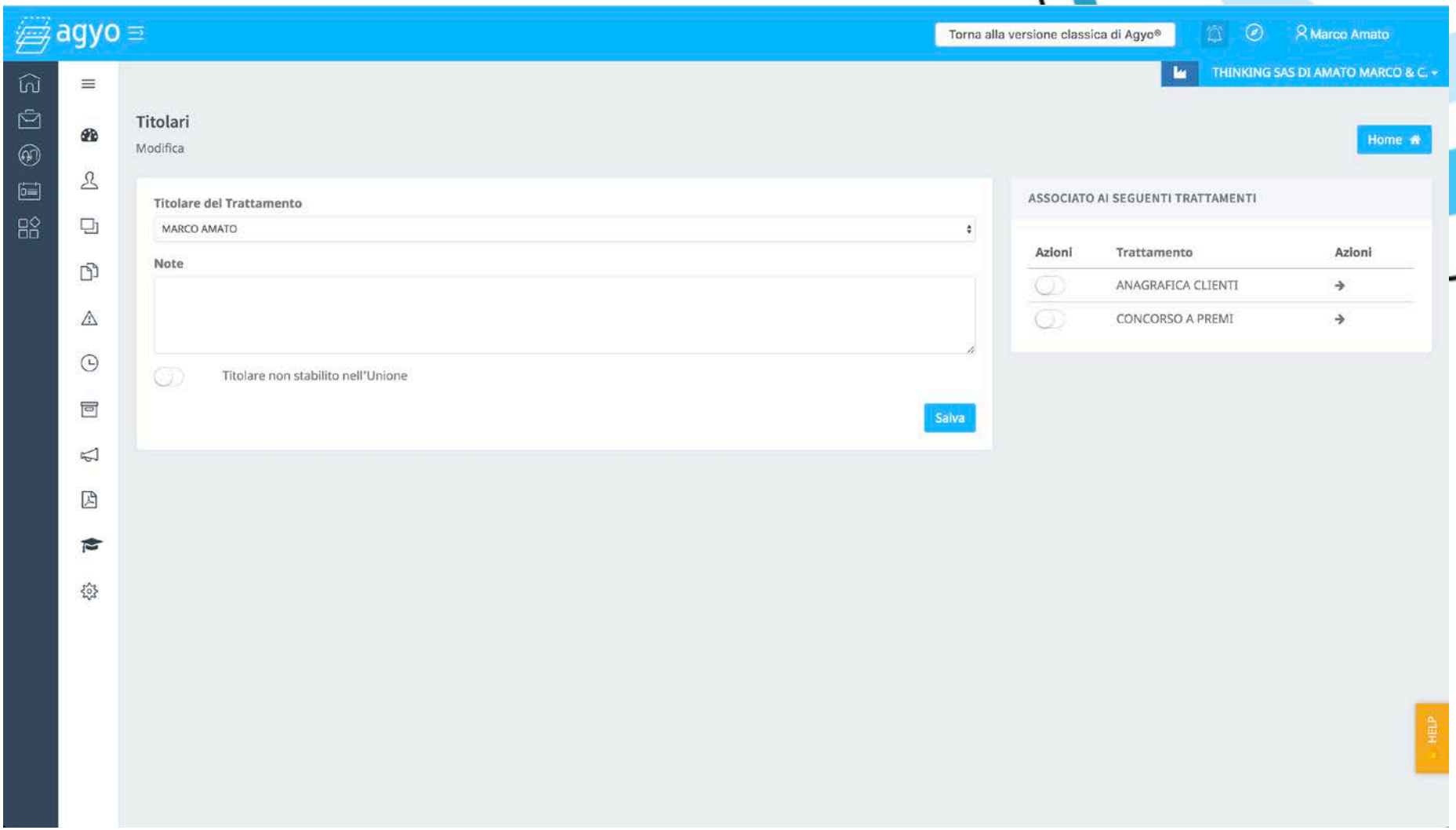
DATA BREACH
Tra i nuovi obblighi, c'è la necessità di comunicare la perdita di dati al Garante della Privacy; grazie a quest'area puoi effettuarlo in modo molto veloce ed organizzato.

REGISTRO DEI CONSENSI
Un archivio per gestire il registro dei consensi raccolti. Tutte le informazioni sono crittografate tramite AES 256.

NORMATIVA
Una comoda area in cui consultare la nuova.

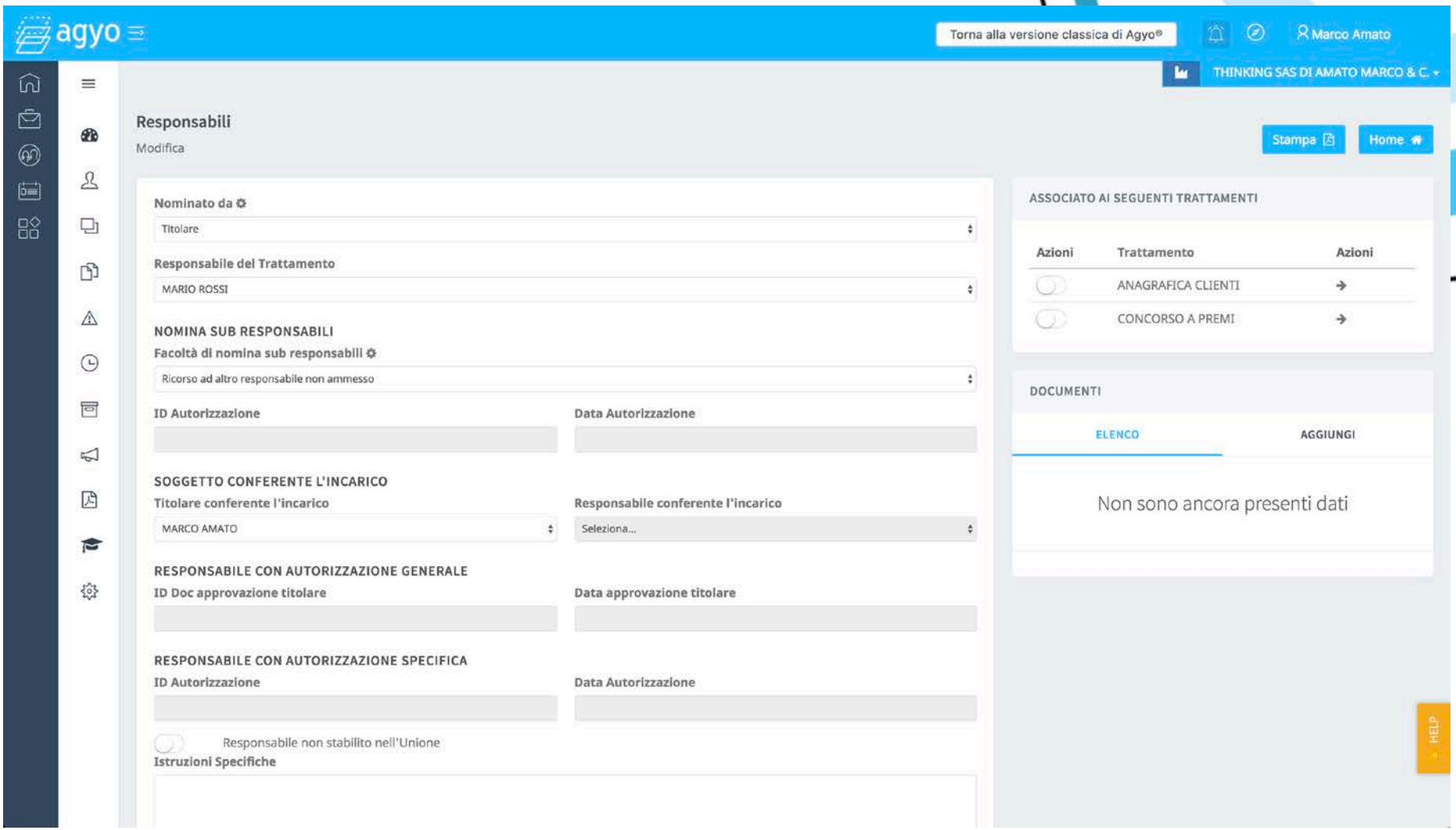
HELP
Il nostro team è pronto ad accogliere le tue richieste di assistenza tramite un sistema di ticketing.

Titolari


agyo
Torna alla versione classica di Agyo®
Marco Amato
THINKING SAS DI AMATO MARCO & C.
Titolari
Modifica
Home
Titolare del Trattamento
MARCO AMATO
Note
Titolare non stabilito nell'Unione
Salva
ASSOCIATO AI SEGUENTI TRATTAMENTI
Azioni
Trattamento
Azioni
ANAGRAFICA CLIENTI
CONCORSO A PREMI
HELP

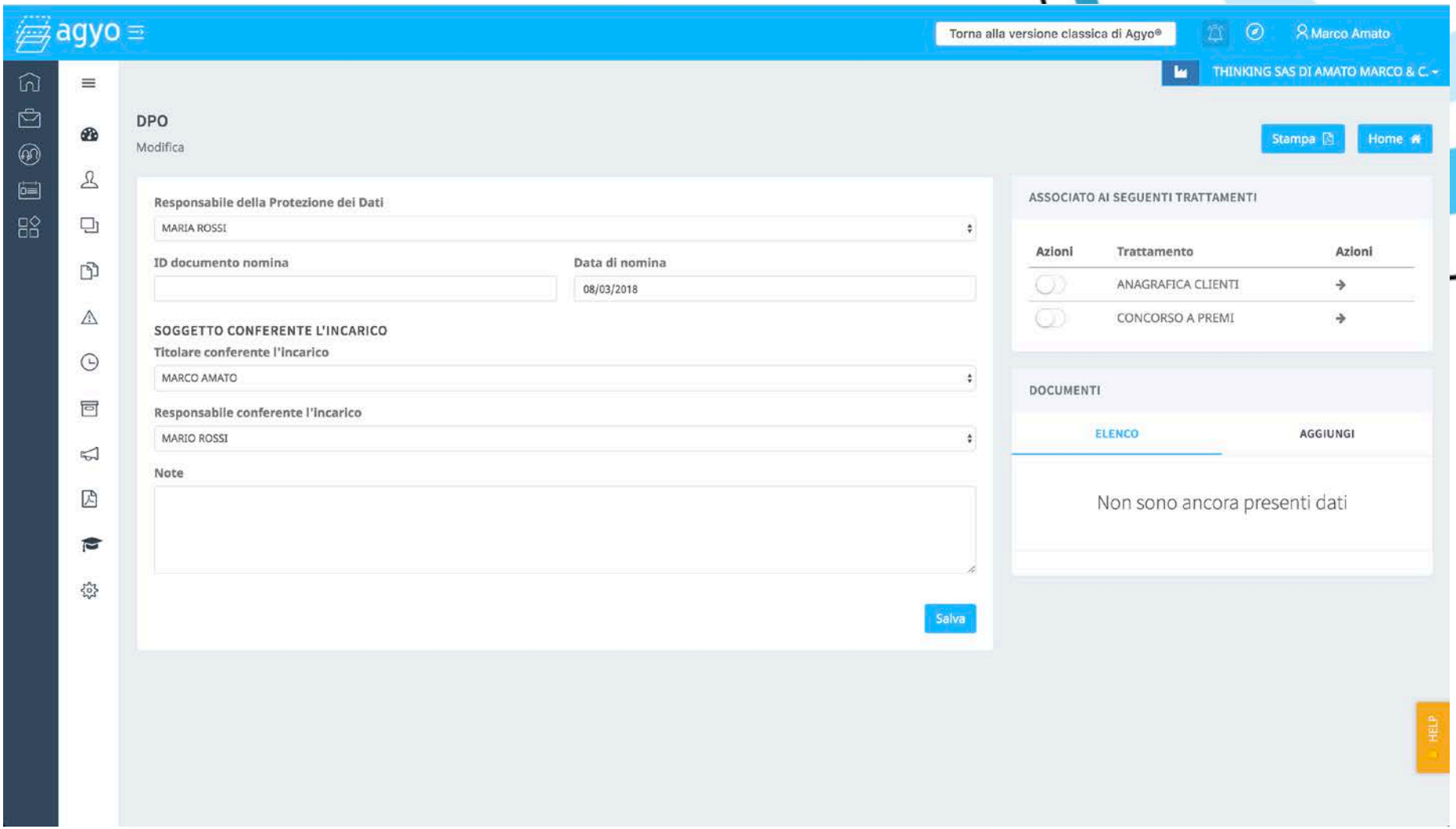
agyo
PRIVACY

Responsabili



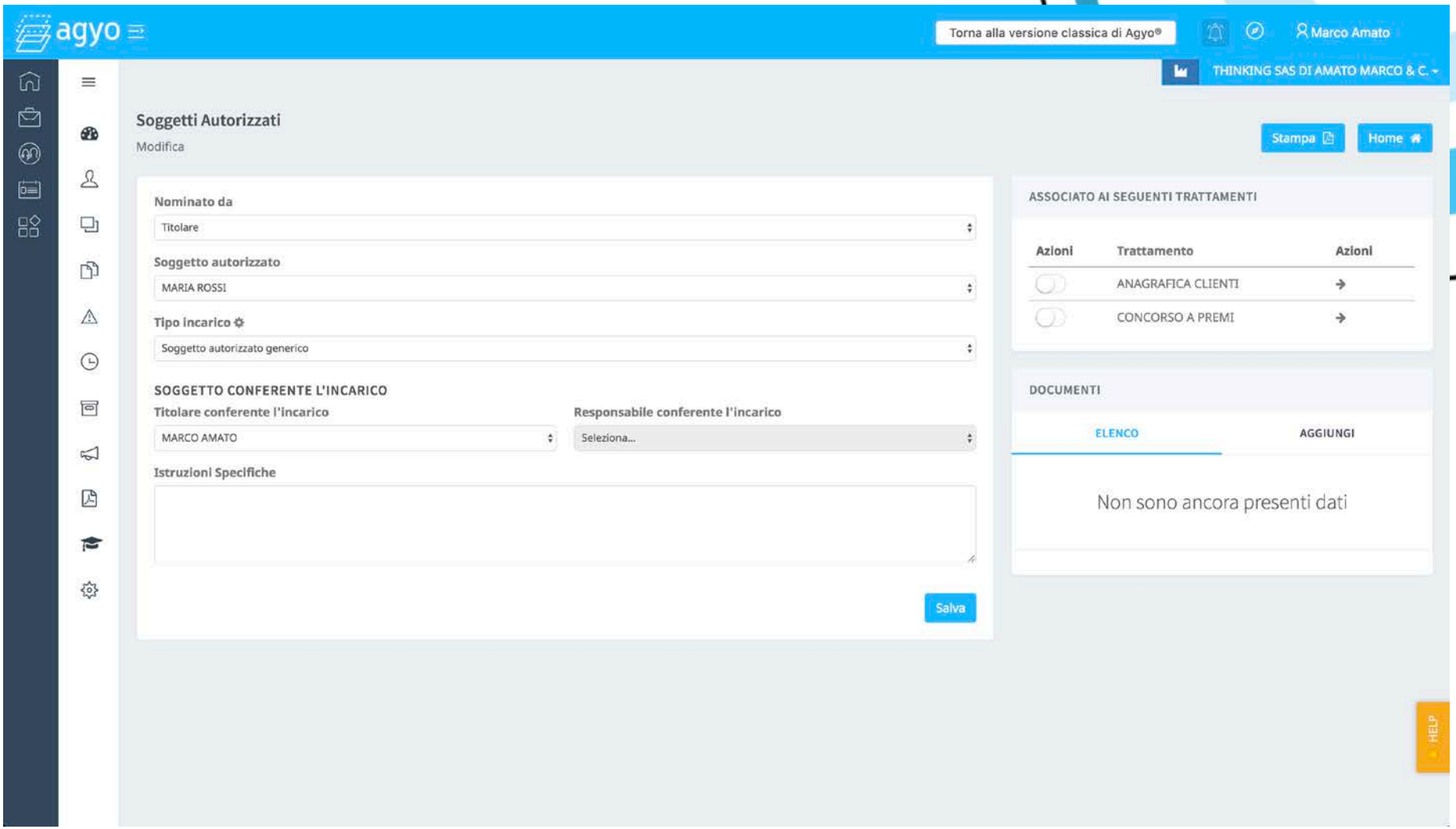
agyo
PRIVACY

DPO



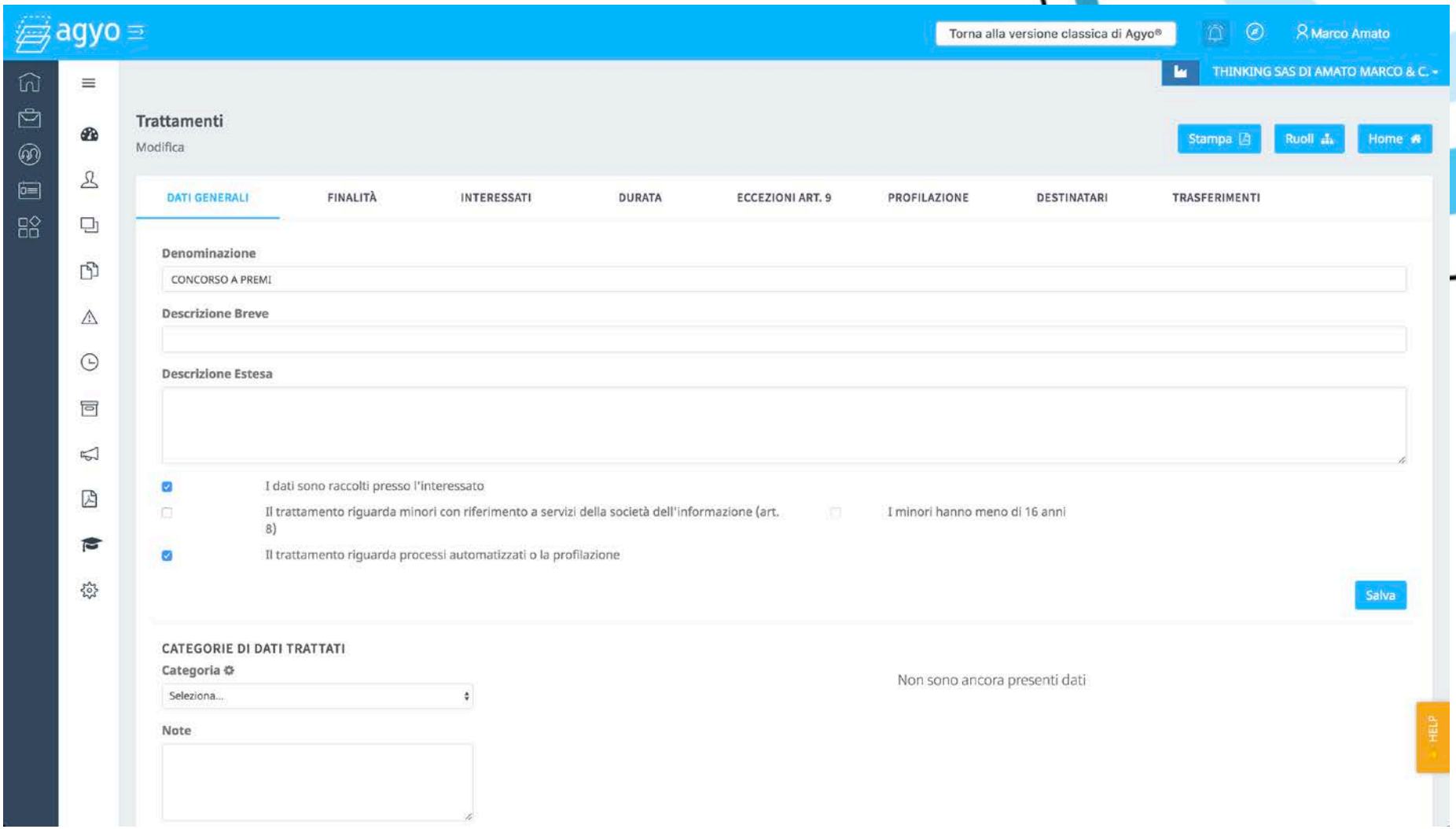
agyo
PRIVACY

Soggetti Autorizzati

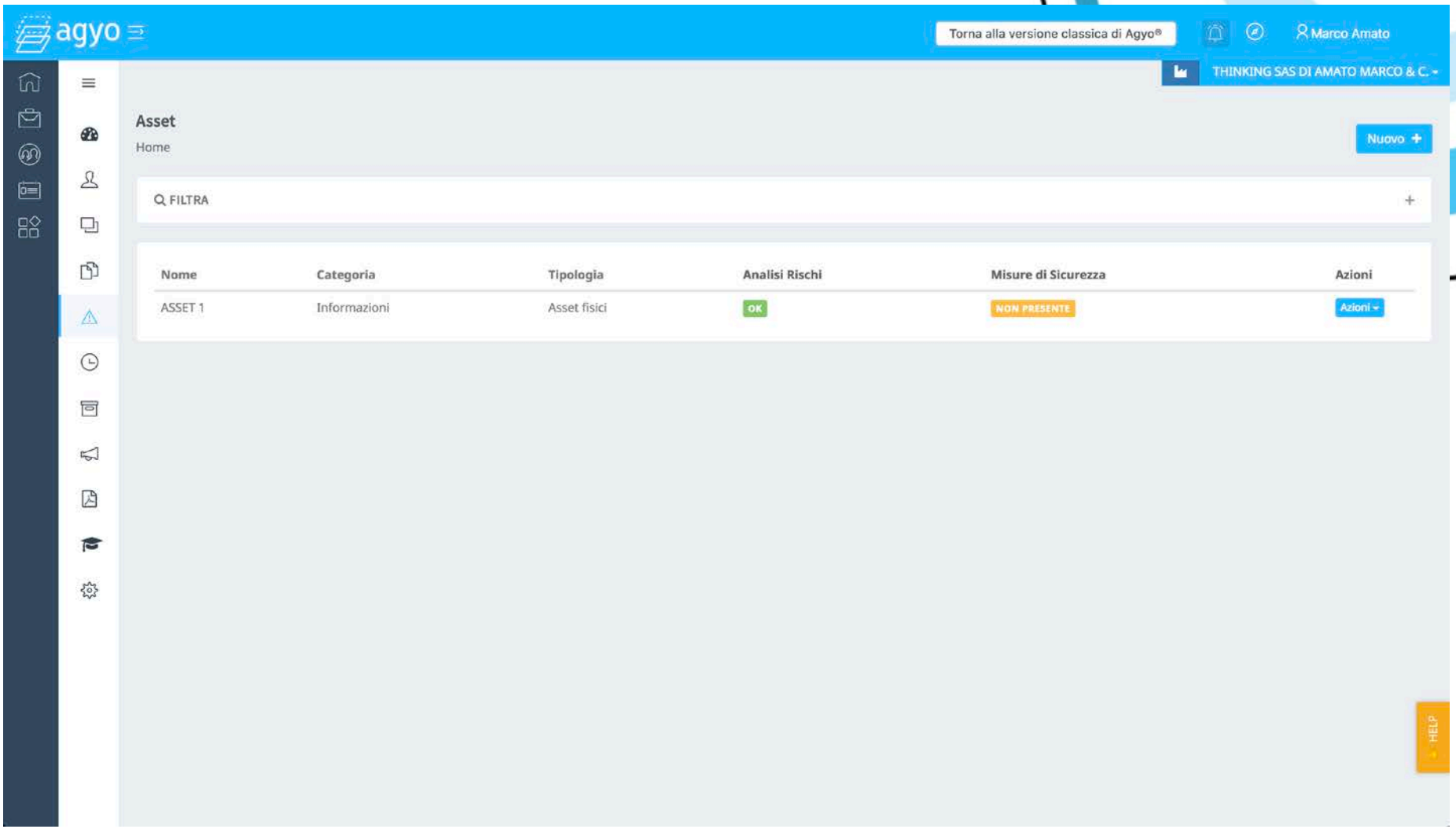


agyo
PRIVACY

Trattamenti

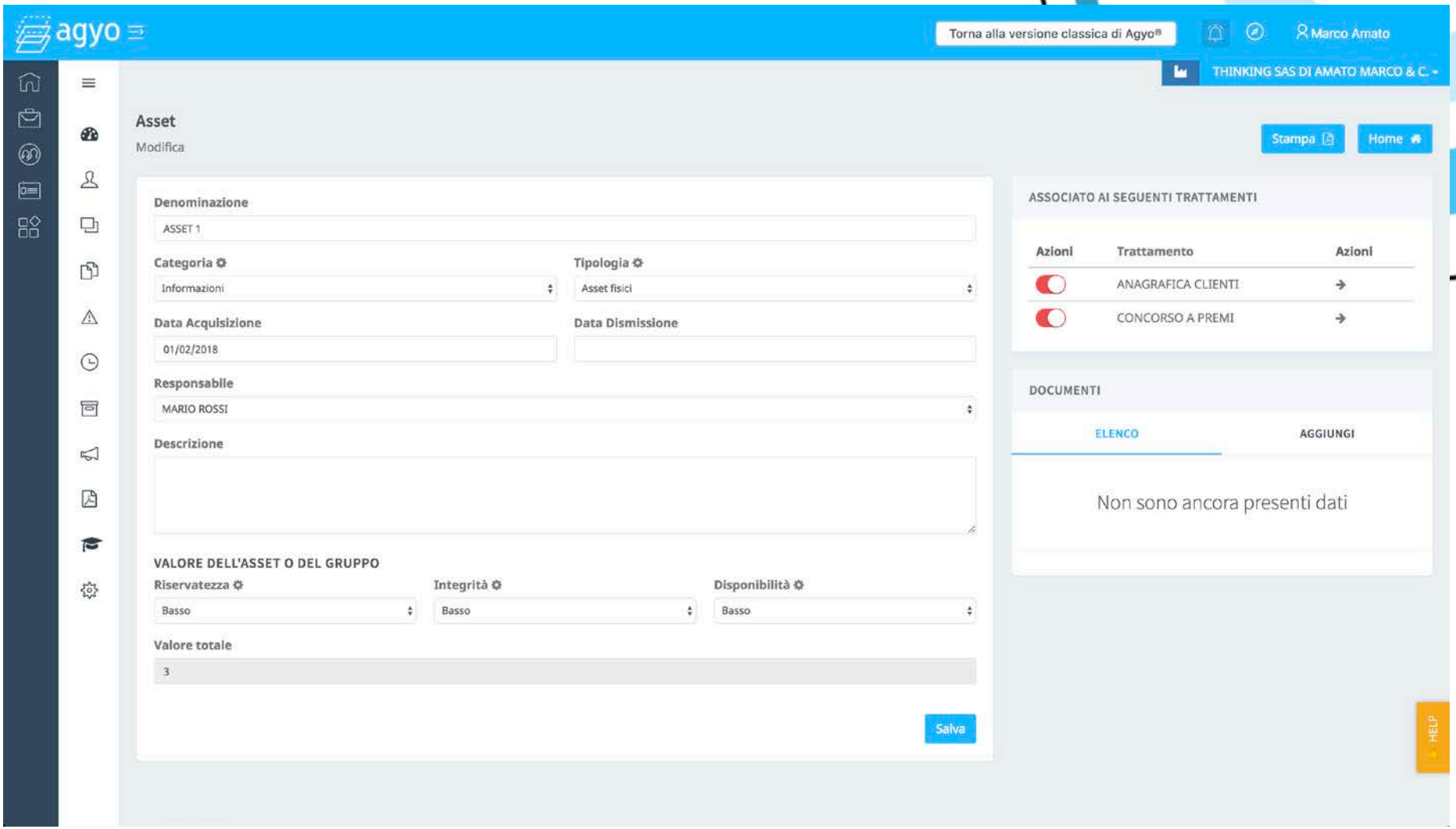


Asset


agyo
Torna alla versione classica di Agyo®
Marco Amato
THINKING SAS DI AMATO MARCO & C.
Asset
Home
Nuovo
FILTRA
Nome
Categoria
Tipologia
Analisi Rischi
Misure di Sicurezza
Azioni
ASSET 1
Informazioni
Asset fisici
OK
NON PRESENTE
Azioni
HELP

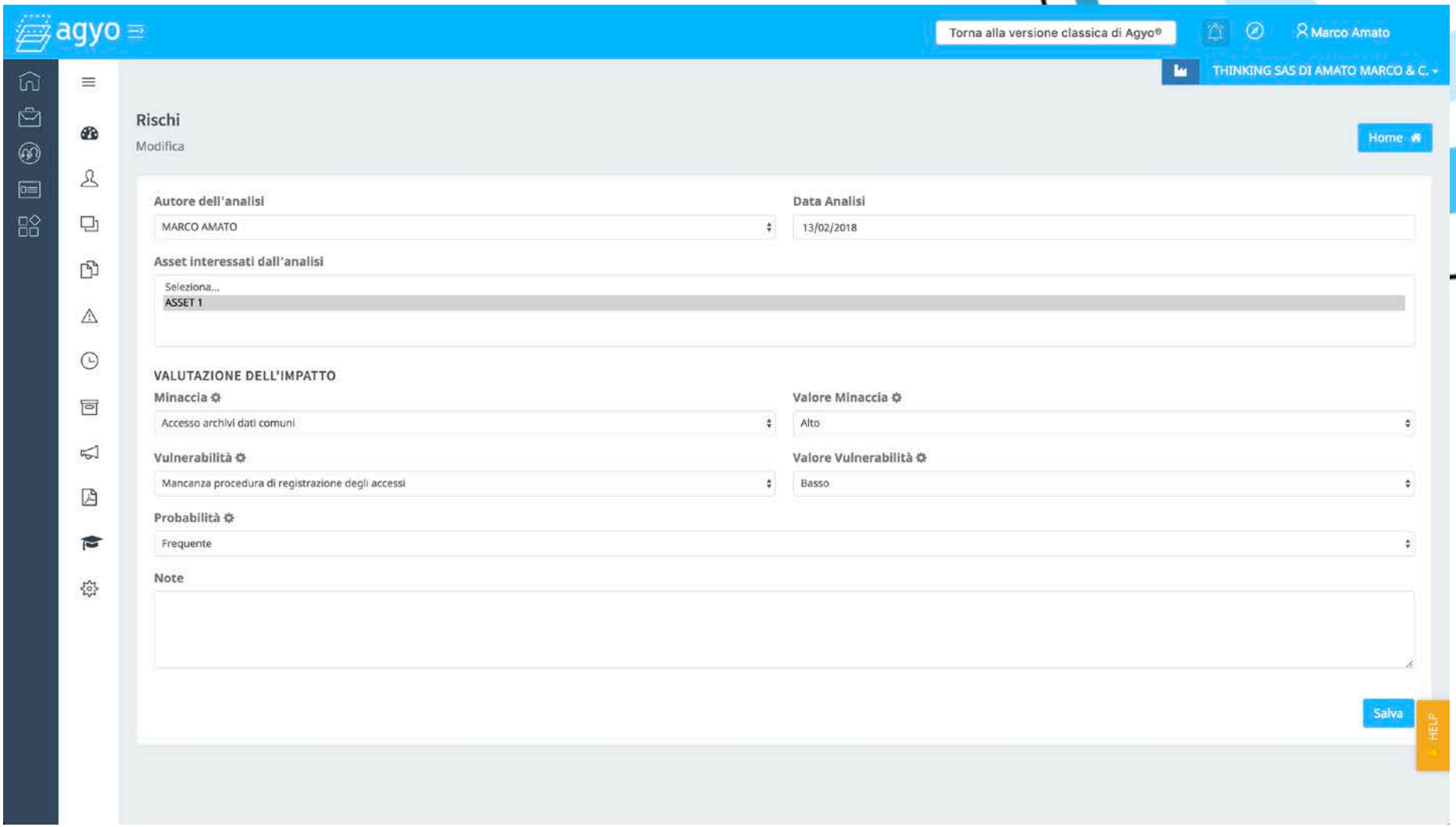
agyo
PRIVACY

Asset



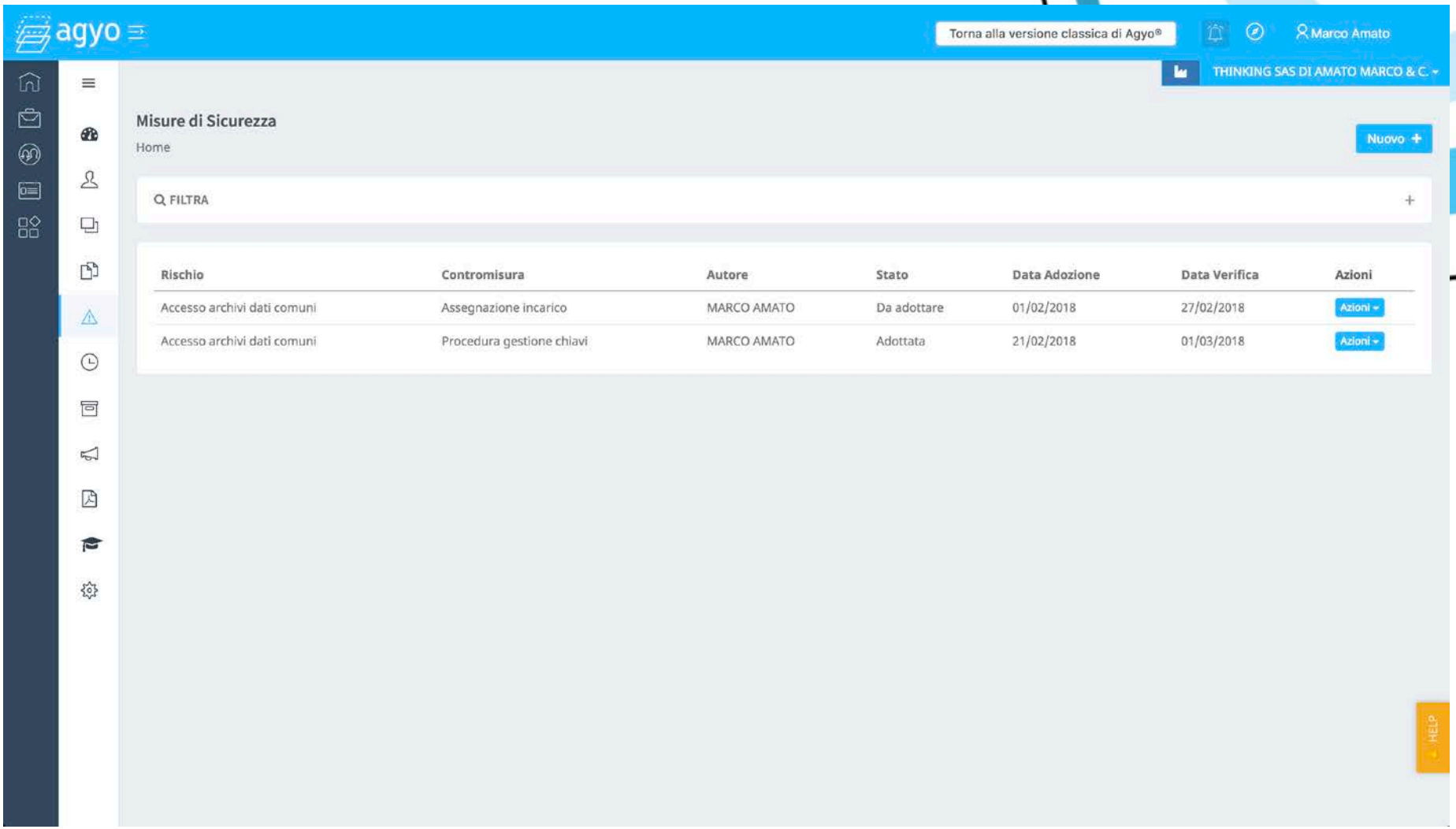
agyo
PRIVACY

Rischi



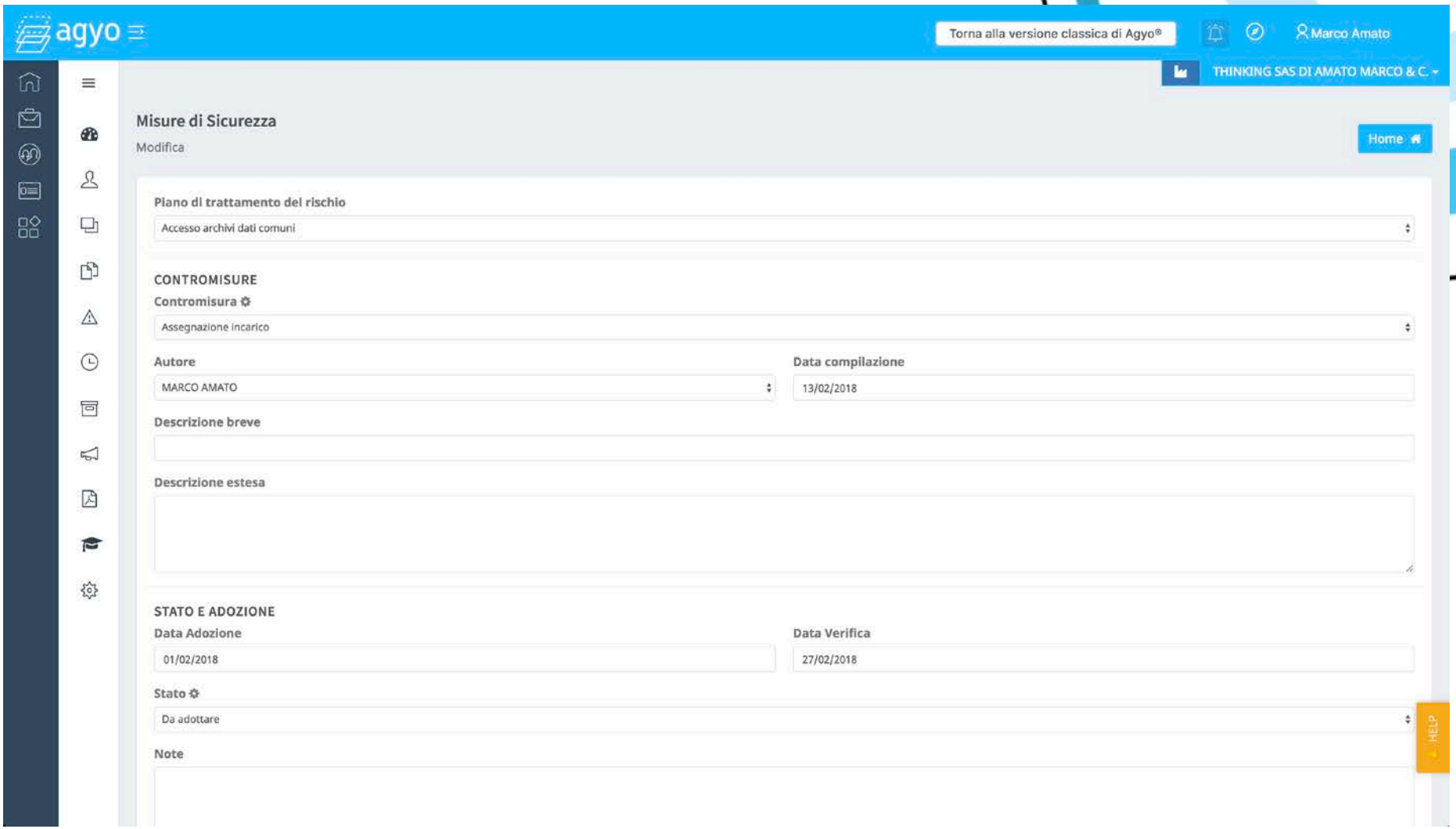
agyo
PRIVACY

Misure di sicurezza



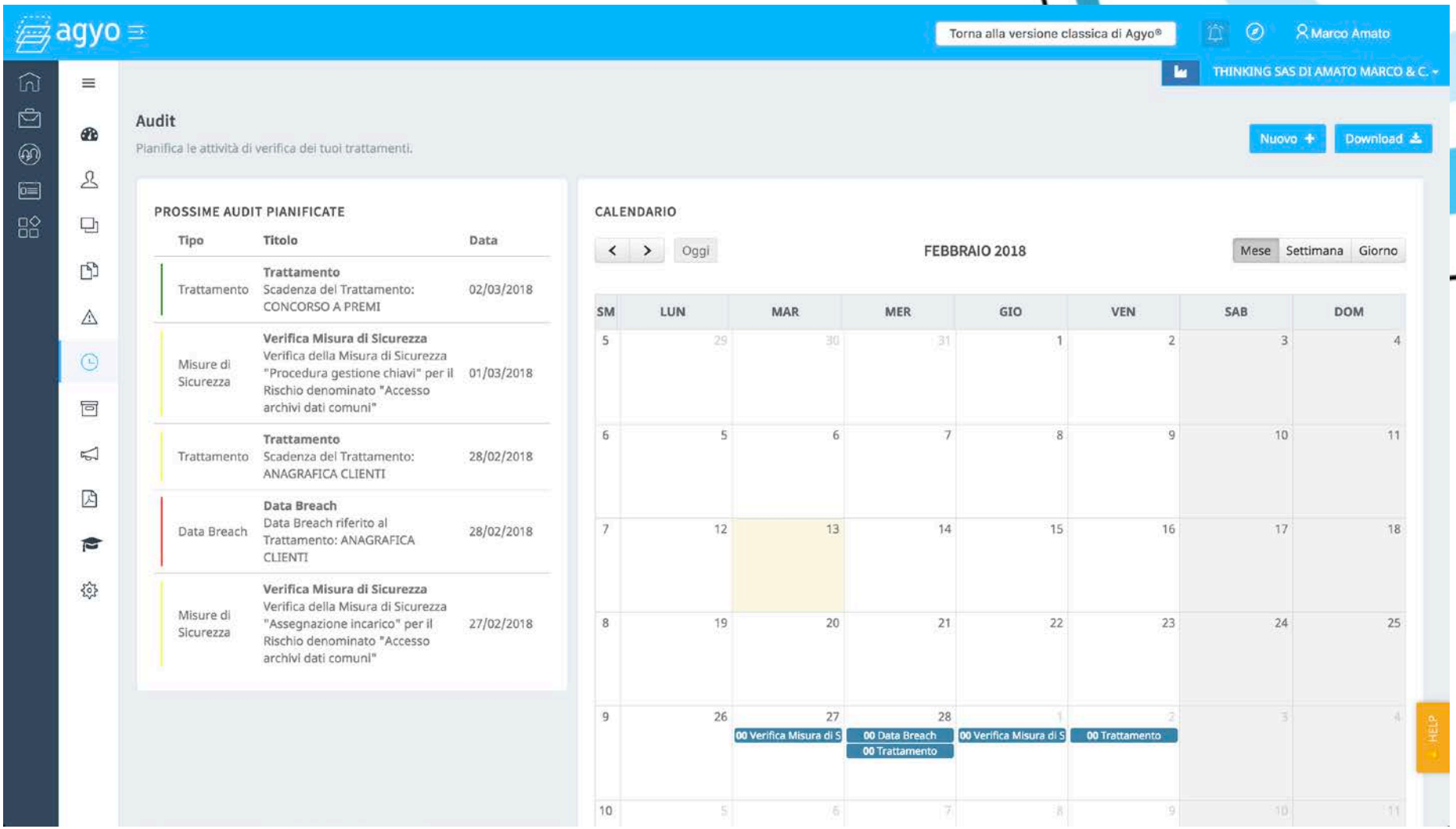
agyo
PRIVACY

Misure di sicurezza



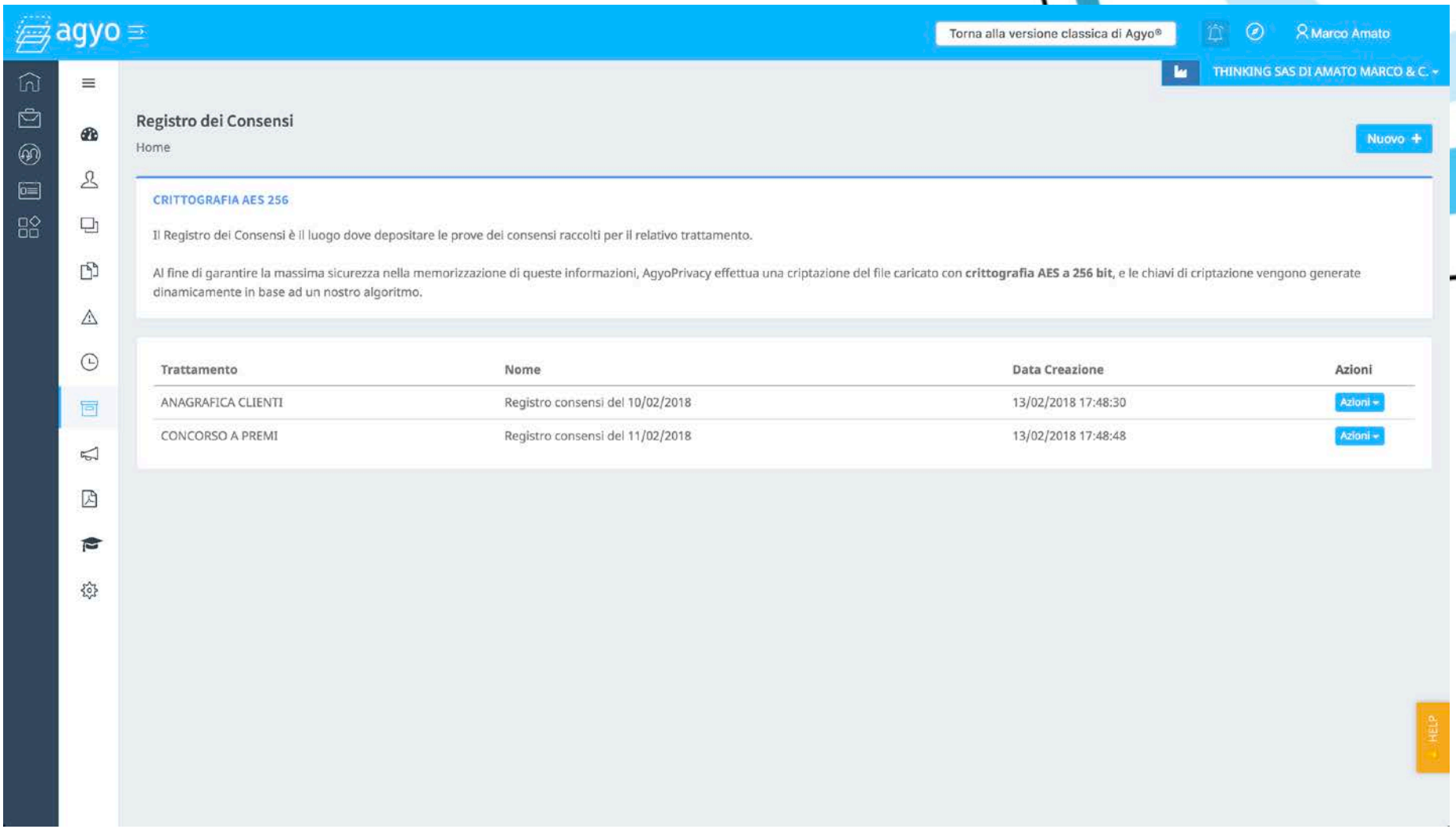
agyo
PRIVACY

Audit



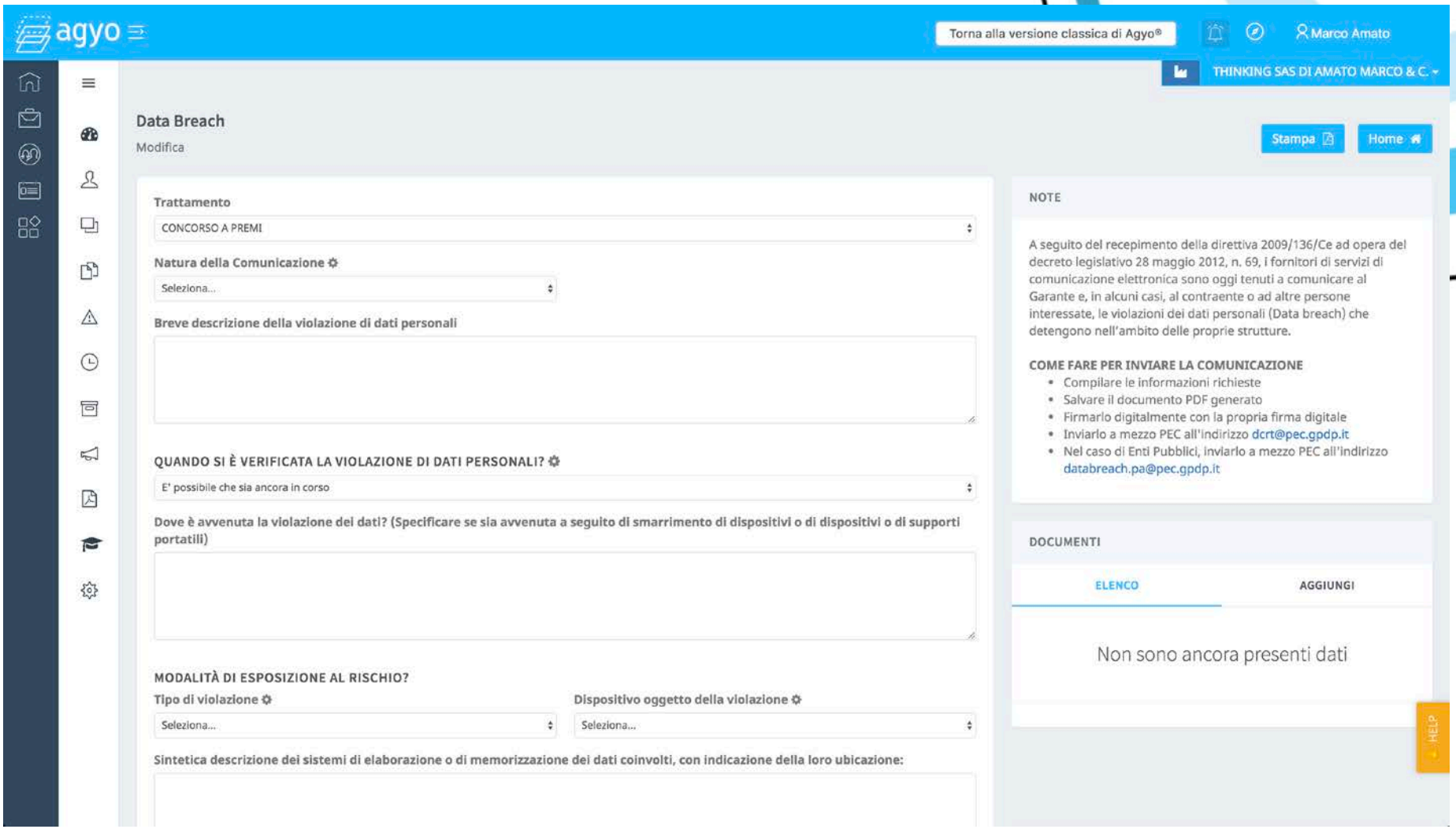
agyo
PRIVACY

Registro dei consensi



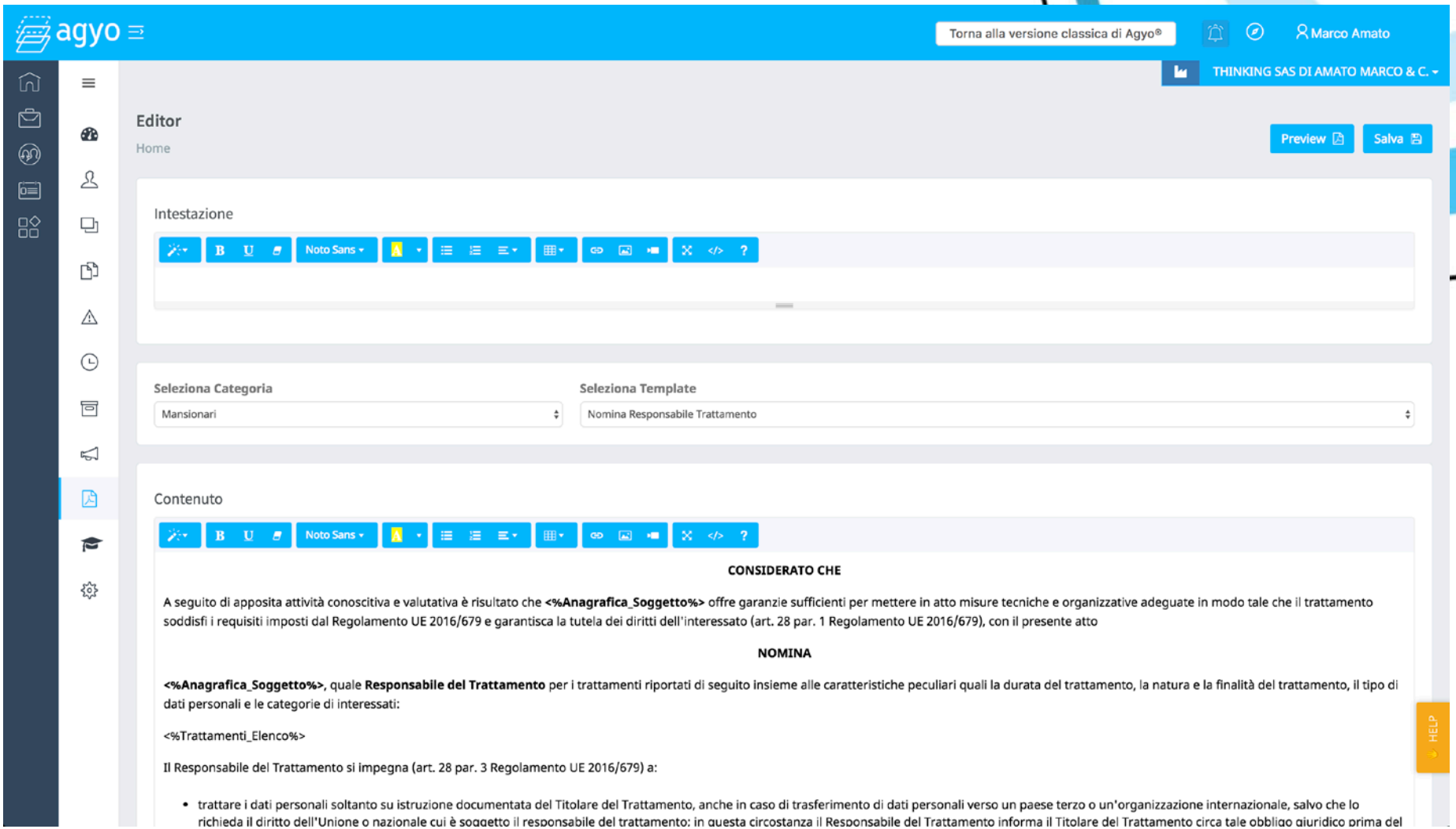
agyo
PRIVACY

Data Breach



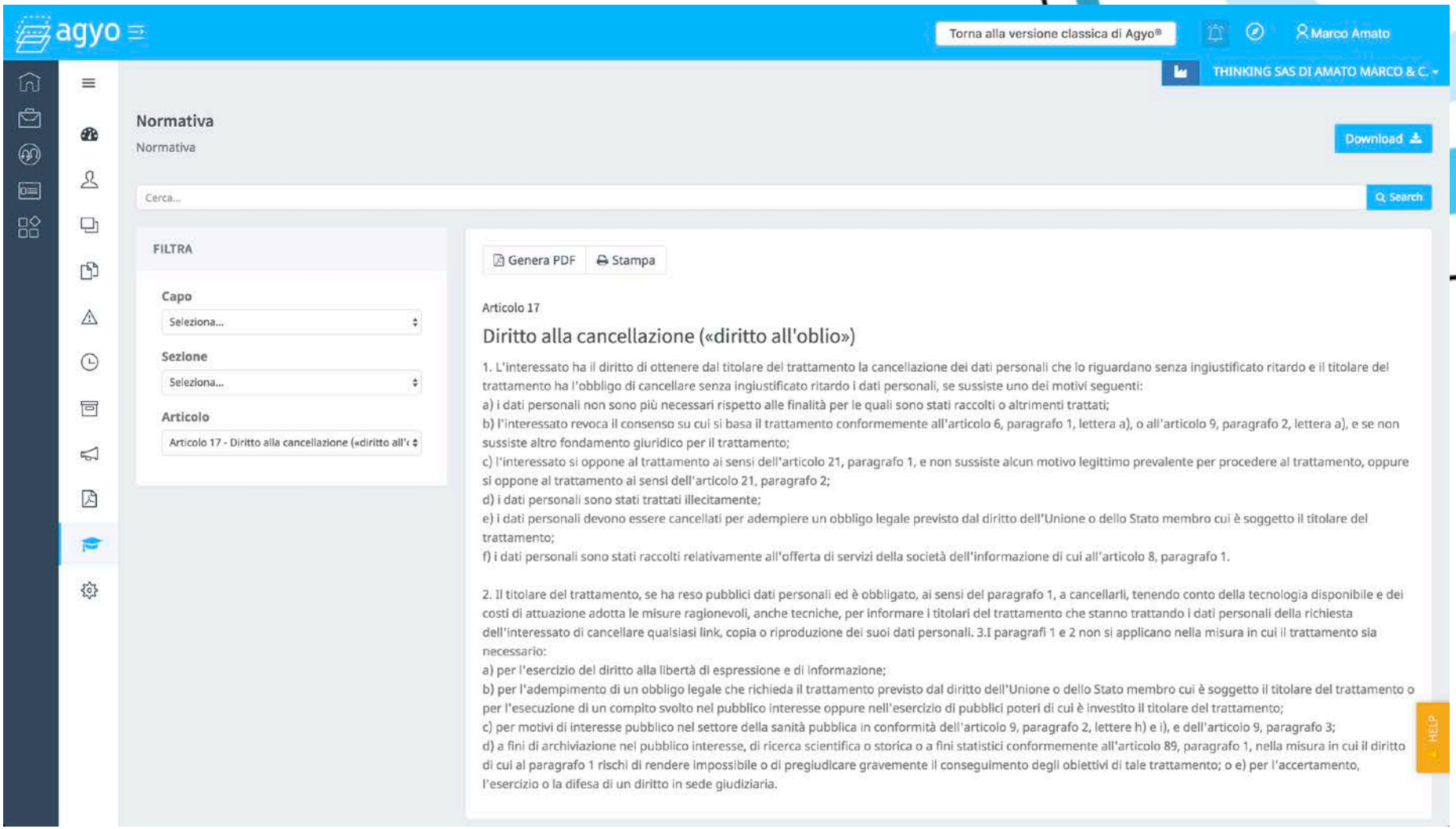
agyo
PRIVACY

Editor



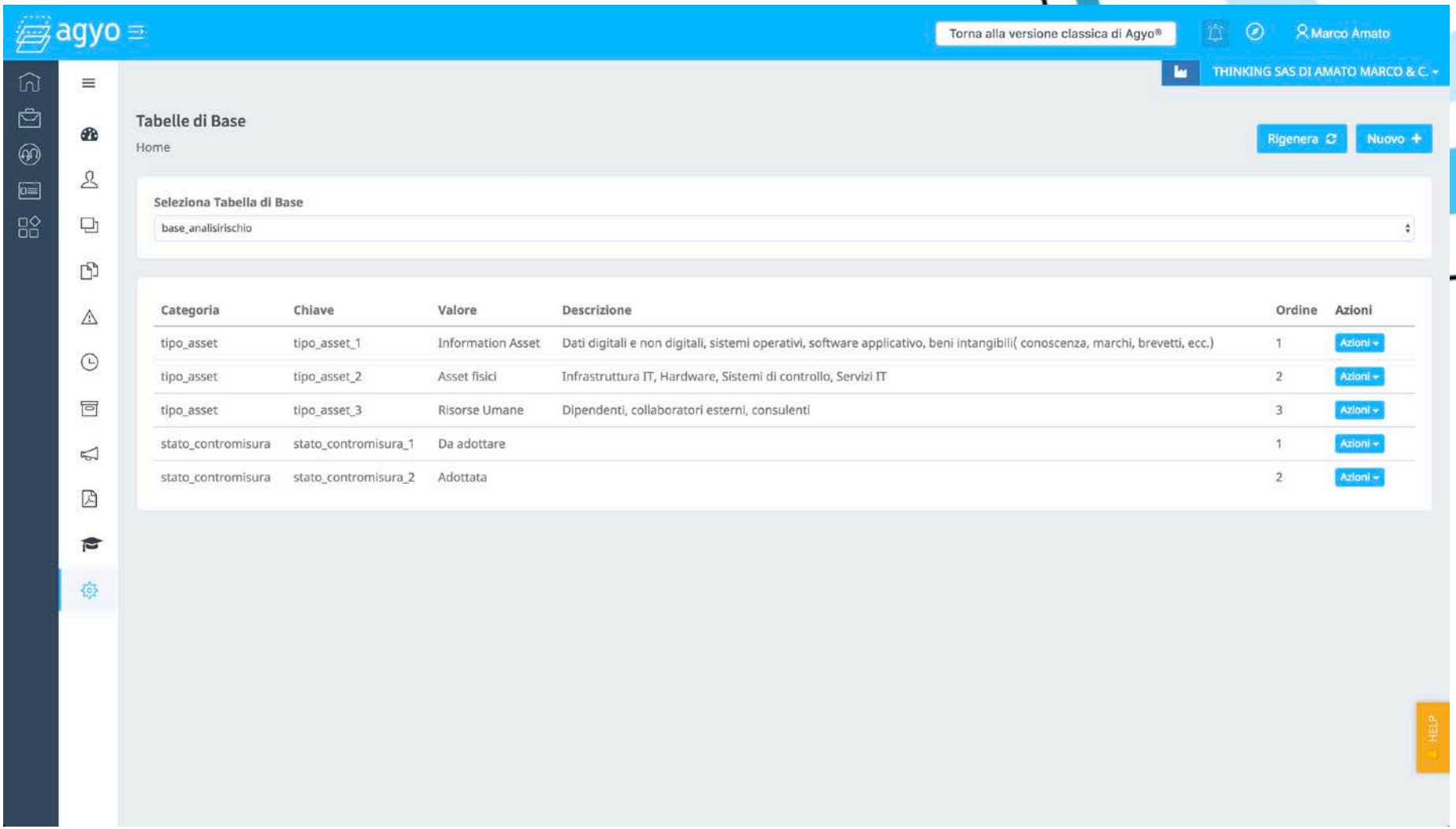
agyo
PRIVACY

Normativa



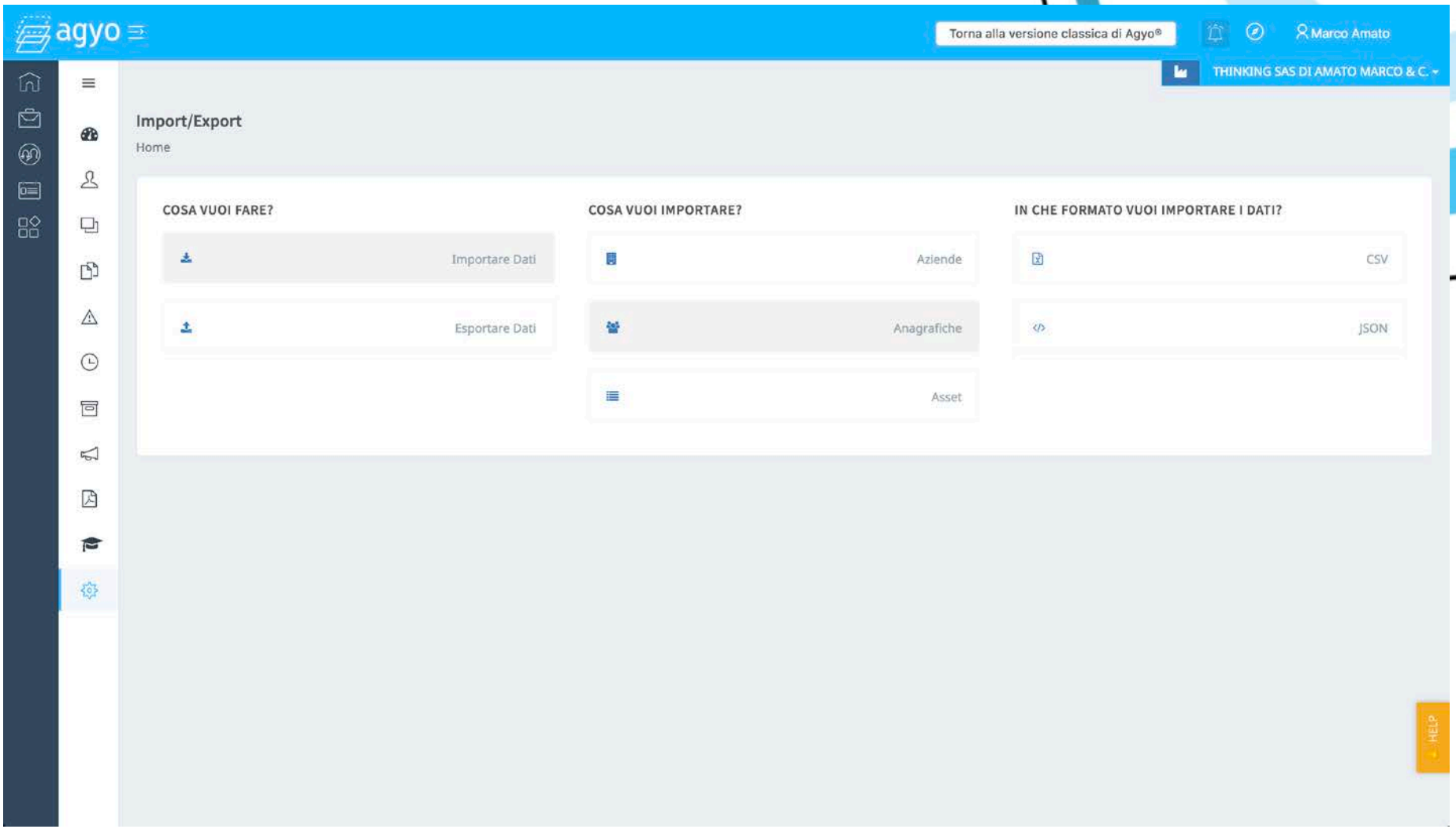
agyo
PRIVACY

Tabelle di Base



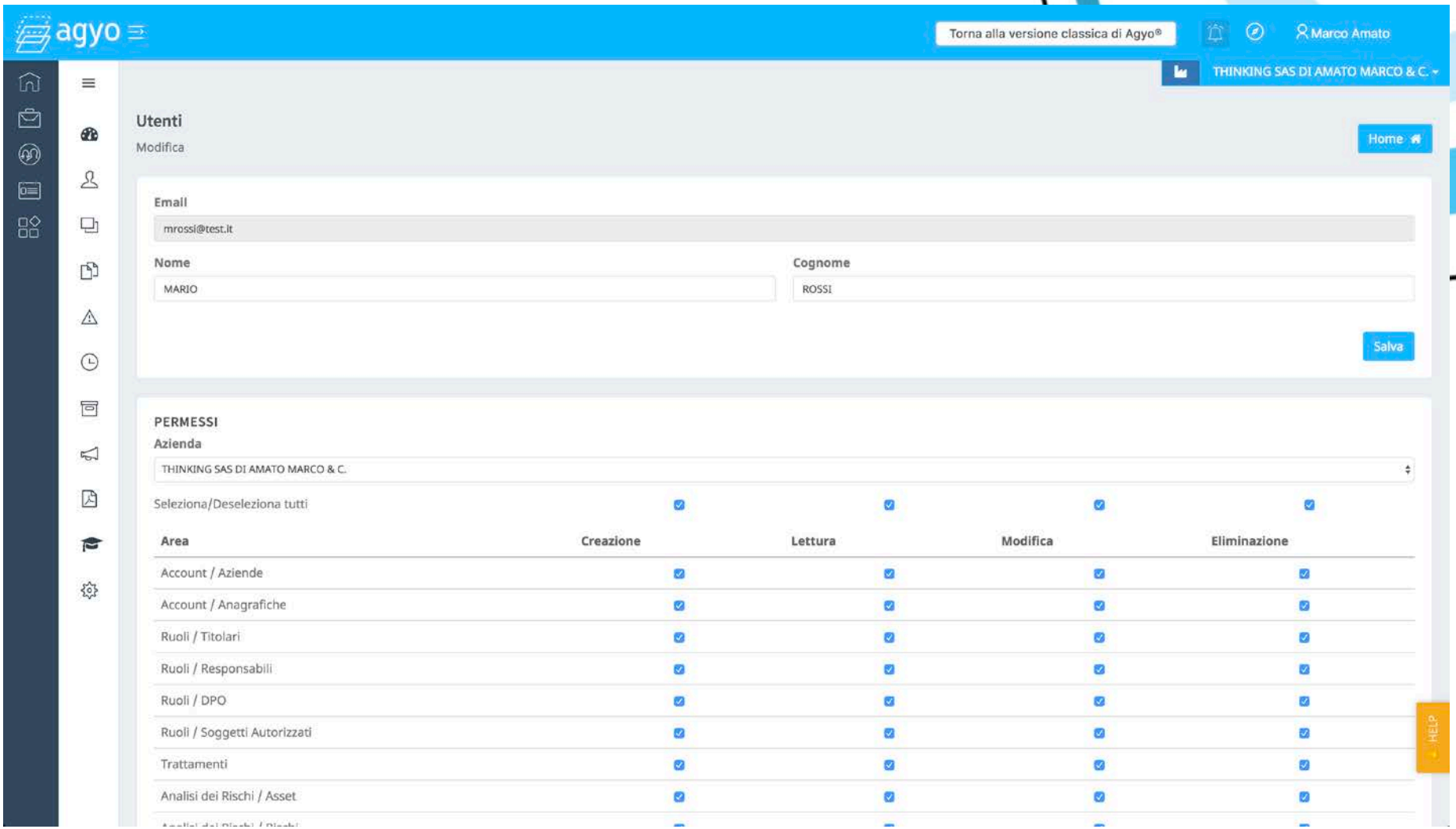
agyo
PRIVACY

Import/Export



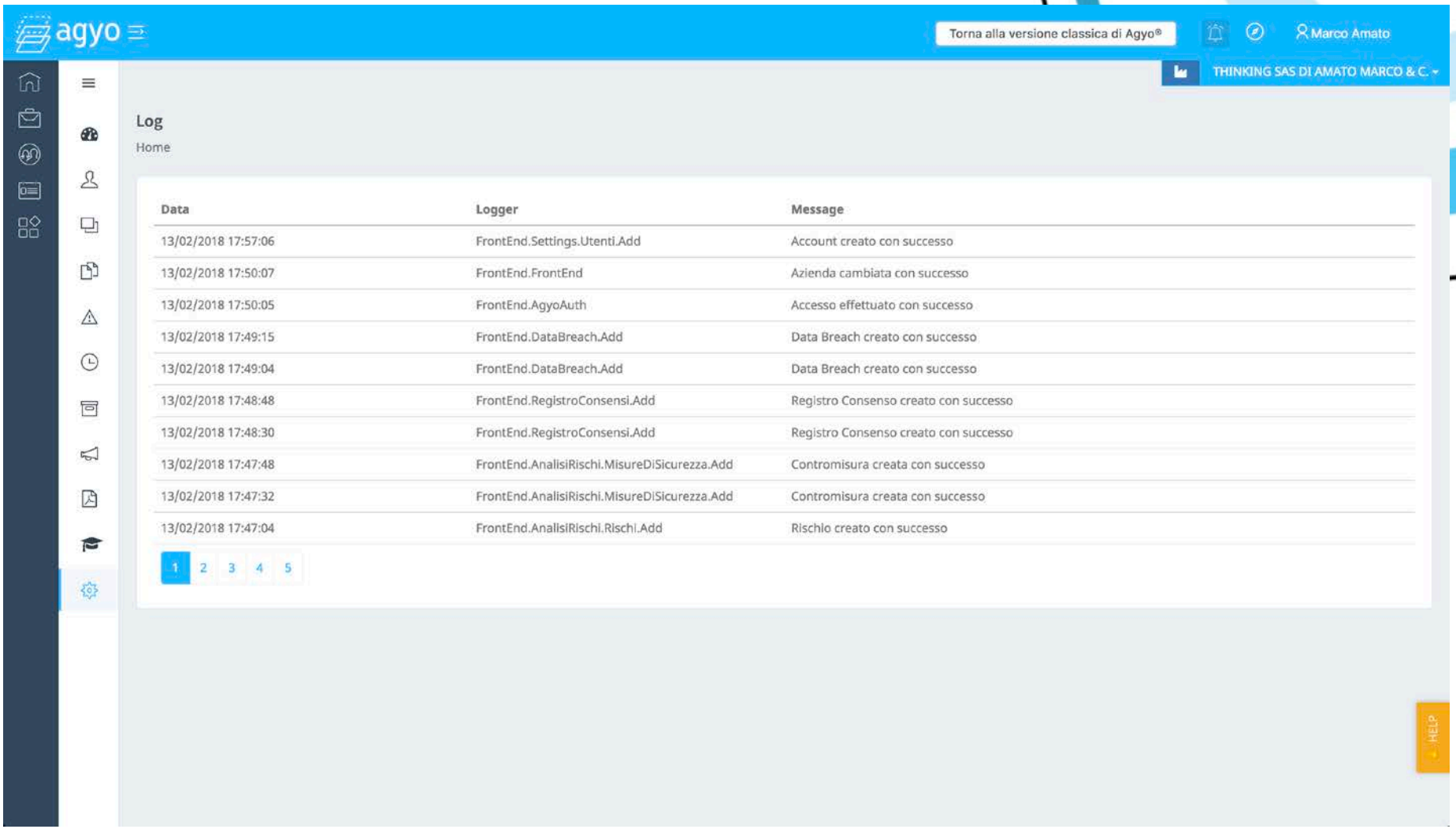
agyo
PRIVACY

Utenti



agyo
PRIVACY

Log

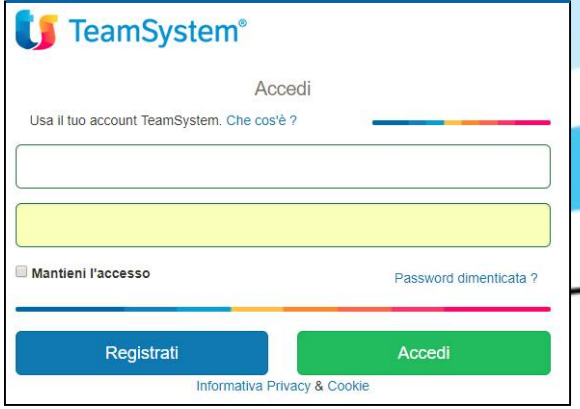


Adeguamento delle soluzioni TeamSystem al GDPR: Privacy by Design e Privacy by Default

Aggiornamento delle procedure Teamsystem legato all'adeguamento normativo obbligatorio al GDPR:

- ✓ **Procedure di autenticazione** finalizzate a consentire **l'identificazione univoca** del soggetto che accede agli applicativi
- ✓ Criteri di **generazione e protezione delle password** conformi alle *best practice* di sicurezza
- ✓ **Funzionalità per il tracciamento dei log degli accessi** e delle attività svolte
- ✓ Misure di ***strong authentication*** **per l'accesso a dati** che richiedono un elevato livello di protezione
- ✓ Funzionalità dirette a consentire **un'attività di monitoraggio** da parte del titolare sull'attività svolta dagli utenti
- ✓ Tecniche di **pseudonimizzazione e crittografia**, in base alla natura dei dati e alle caratteristiche del trattamento

TEAMSYSTEM ID



LOG MANAGEMENT

Integrazione gestionali TeamSystem con AGYO Privacy per archiviazione e consultazione dei log

DATI CRIPTATI

Criptazione dei dati sensibili presenti negli archivi delle soluzioni gestionali

CONSENSO INTERESSATI

Conservazione in AGYO Privacy dei consensi generati negli applicativi gestionali.

AGYO PRIVACY

GDPR senza pensieri?
Scegli il software in cloud Agyo Privacy

GRUPPO progetto studio

TeamSystem®