



Scheda informativa

Informazioni per avvocature sulla sicurezza e protezione dei dati nell'utilizzo della piattaforma justitia.swiss

Questa scheda informativa si rivolge alle avvocate e agli avvocati e agli studi legali che utilizzano la piattaforma justitia.swiss per la comunicazione elettronica con le autorità giudiziarie. Illustra gli aspetti principali di sicurezza delle informazioni e di protezione dei dati nell'utilizzo della piattaforma e risponde alle domande più frequenti in fatto di responsabilità, misure di sicurezza e condizioni quadro organizzative. Justitia 4.0 mette a disposizione una serie di misure tecniche e organizzative atte a proteggere la trasmissione e l'elaborazione di dati. Determinati compiti e responsabilità, invece, rimangono di competenza delle avvocate, degli avvocati e degli studi legali collegati. L'obiettivo della presente scheda informativa è di aiutare a meglio comprendere quali sono le diverse competenze e come utilizzare la piattaforma in sicurezza.

1 Chi è responsabile della sicurezza delle informazioni e della protezione dei dati nell'utilizzo della piattaforma justitia.swiss?

La responsabilità della sicurezza delle informazioni e della protezione dei dati è suddivisa fra la piattaforma justitia.swiss e le avvocate, gli avvocati e gli studi legali collegati. A Justitia 4.0 compete la responsabilità per la sicurezza d'esercizio della piattaforma e per le misure di sicurezza tecniche e organizzative implementate a tal riguardo. Questo comprende in particolare l'autenticazione e l'autorizzazione degli utenti, la cifratura dei dati, la registrazione degli eventi rilevanti per la sicurezza e l'emissione di ricevute e credenziali. Le avvocate, gli avvocati e gli studi legali collegati mantengono la responsabilità per la sicurezza della propria organizzazione e dei propri sistemi locali. Questo comprende in particolare la gestione dei conti utente e delle autorizzazioni, la protezione dell'infrastruttura IT locale, il backup di dati nel proprio ambiente e la sensibilizzazione dei collaboratori sulla sicurezza delle informazioni e sulla protezione dei dati.

2 Quali requisiti si applicano alle identità digitali e all'accesso alla piattaforma?

L'accesso alla piattaforma avviene attraverso identità digitali affidabili. Nel caso di persone fisiche, AGOV è la soluzione di autenticazione più indicata. Possono essere utilizzati anche altri fornitori di identità (Identity Provider) supportati dalla piattaforma. L'autenticazione avviene attraverso il rispettivo Identity Provider e non sulla piattaforma. Per utilizzare la piattaforma le avvocate e gli avvocati devono essere in possesso di un'identità digitale valida e seguire la prevista procedura di autenticazione. I dati di accesso e i mezzi di autenticazione devono essere protetti adeguatamente e non divulgati a terzi. Gli studi legali dovrebbero assicurarsi di assegnare le identità digitali esclusivamente alle persone autorizzate e di aggiornarle tempestivamente nel caso di cambiamenti di personale o di funzione. Bisogna inoltre rimuovere immediatamente i diritti di accesso obsoleti.

3 Quali requisiti si applicano alle firme e alle credenziali elettroniche?

La comunicazione elettronica attraverso la piattaforma è regolata dalle disposizioni di legge vigenti. Le firme elettroniche servono per garantire la provenienza e l'integrità dei documenti inoltrati elettronicamente. Durante l'esercizio pilota, i requisiti applicabili possono divergere dalle disposizioni previste in futuro con la LCEG. Con l'entrata in vigore completa della LCEG le disposizioni di legge in materia di comunicazione elettronica in ambito giudiziario diventano vincolanti. La piattaforma emette ricevute e credenziali a sostegno della tracciabilità degli inoltri e delle notificazioni elettronici. Ciò permette di documentare il momento di trasmissione di un inoltrato o di ricezione di una notificazione. Le avvocate e gli avvocati dovrebbero assicurarsi che vengano rispettate le disposizioni applicabili ai loro procedimenti riguardo a firme e credenziali elettroniche. Ulteriori informazioni in merito sono fornite nella documentazione sulla piattaforma.

4 Come vengono protetti i documenti e i dati sulla piattaforma?

La piattaforma justitia.swiss adotta diverse misure di sicurezza tecniche e organizzative allo scopo di garantire la riservatezza, l'integrità e la tracciabilità dei documenti e dei dati trasmessi. Le trasmissioni sono effettuate esclusivamente attraverso collegamenti cifrati. I file sono memorizzati in modo sicuro e sono protetti da accessi non autorizzati attraverso meccanismi di protezione supplementari.

Durante il caricamento di documenti, i formati di file supportati sono automaticamente soggetti a verifiche. Fra queste si citano la verifica del formato di file e le misure di protezione ai fini di rilevamento di malware. I file caricati sono inoltre muniti di credenziali di integrità ai fini di tracciabilità delle modifiche effettuate ai documenti.

La piattaforma registra gli eventi rilevanti per la sicurezza ed emette ricevute e credenziali per le operazioni rilevanti. Questo permette anche in un secondo tempo di tracciare le notificazioni elettroniche e altre attività importanti.

Solo gli utenti e le organizzazioni debitamente autorizzati possono accedere ai documenti e ai dati. I diritti di accesso sono assegnati e verificati nel quadro dei ruoli e delle autorizzazioni definiti nella piattaforma.

5 Quali requisiti si applicano agli studi legali?

L'utilizzo della piattaforma non esonera gli studi legali dalla loro responsabilità di realizzare adeguate misure di sicurezza organizzative e tecniche all'interno della propria organizzazione. Gli studi legali sono responsabili della sicurezza dei propri sistemi IT locali, reti e postazioni di lavoro. Dovrebbero anche assicurare di verificare regolarmente i conti utente e le autorizzazioni e di aggiornarli tempestivamente nel caso di cambiamenti organizzativi. In particolare in caso di arrivi e partenze di personale bisogna rimuovere immediatamente i diritti di accesso obsoleti. Inoltre andrebbero attuate misure opportune di backup e ripristino di dati. Ciò vale in particolare per documenti e informazioni che vengono scaricati dalla piattaforma o elaborati fuori dalla piattaforma. Si raccomanda di sensibilizzare regolarmente i collaboratori sui temi legati alla sicurezza delle informazioni e alla protezione dei dati. Ciò comprende in particolare l'utilizzo sicuro delle identità digitali, il rilevamento di tentativi di phishing e la protezione di informazioni riservate.

Ulteriori informazioni

Ulteriori informazioni e informazioni su argomenti correlati possono essere ottenute scrivendo a info@justitia.swiss e/o consultando il sito web www.justitia40.ch.