Urano4Web

Gea di Fioretti Massimiliano SAS & C.
Via dei Gemelli, 7 – 00040 Ardea (RM)
C.F. e P.I. 11101001003
Telefono 06.9179258
Fax 06.45501935
Email: info@gea-software.com

Revisione del 23 Marzo 2018

Attestazione dei requisiti del Sistema

Protezione dei dati personali

(ex GDPR – REG. UE 2016/679)

Il sottoscritto Massimiliano Fioretti, in qualità di Legale Rappresentante della GEA di Fioretti Massimiliano SAS & C. (di seguito GEA), titolare della produzione, commercializzazione (con concessione di licenza d'uso) e gestione del Software Urano4web (di seguito Il Software), con la presente illustra le caratteristiche di protezione e sicurezza del Software alla versione 5.9, dichiarandolo pienamente rispondente ai requisiti necessari per la corretta applicazione del Regolamento UE 2016/679 (di seguito GDPR) da parte degli utilizzatori.

Il Sistema integra i principi ***privacy by design*** e ***privacy by default previsti dall'Art. 25 del GDPR***, essendo stato concepito e sviluppato, sin dalla progettazione, come un ambiente operativo in cui il trattamento dei dati avviene unicamente se necessario, in modo limitato e funzionale ai profili di attribuiti ai singoli utenti, con adeguate protezioni, atte a evitare rischi per la riservatezza, l'integrità e la disponibilità dei dati stessi.

Il Sistema permette di modificare le configurazioni e aggiungere istruzioni operative specifiche, in funzione delle particolarità organizzative e del trattamento effettuato da ciascun titolare.

Nella progettazione del Software, è stato tenuto conto della particolare natura dei dati trattati, tipicamente consistenti in *dati personali particolari relativi alla salute dei lavoratori*, ed è stata condotta una specifica valutazione per individuare i rischi per i diritti e le libertà fondamentali dei lavoratori con riguardo al trattamento dei dati personali. La valutazione ha tenuto conto di valori quali la dignità umana, gli interessi legittimi e i diritti fondamentali dei lavoratori, in particolare per quanto riguarda la trasparenza del trattamento e i sistemi di monitoraggio sul posto di lavoro.

Dall'analisi condotta sono stati individuati i rischi per la loro riservatezza, che possano derivare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale dei dati trattati.

La medesima valutazione ha tenuto conto della tecnologia utilizzata per il trattamento, per l'archiviazione e per la trasmissione dei dati.

Gea di Fioretti Massimiliano SAS & C.
Via dei Gemelli, 7 – 00040 Ardea (RM)
C.F. e P.I. 11101001003
Telefono 06.9179258
Fax 06.45501935
Email: info@gea-software.com

Con riferimento all'art. 32 *(Sicurezza del Trattamento)* del citato Regolamento, l'utilizzo del software permette l'efficace protezione dei dati personali, consentendo l'applicazione di misure tecniche ed organizzative adeguate per garantire un elevato livello di sicurezza ed in particolare:

a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) la definizione ed applicazione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento.

I punti C e D sono automaticamente presenti nelle versione Server Cloud. Per le versioni Locale e Server Lan, il software si limita a dare la possibilità di adottare le misure di sicurezza che, tuttavia, sono determinate dall'infrastruttura sulla quale il software è installato.

Nel merito e a testimonianza di quanto sopra dichiarato, si riporta una sintesi delle caratteristiche e dei dettagli funzionali di Urano4Web:

SPECIFICHE DEL SOFTWARE

1. DESTINATARI DEL TRATTAMENTO (TITOLARI O RESPONSABILI)
   Il software è rivolto in particolare a:

   - Singoli Medici Competenti
   - Piccole, medie e grandi aziende
   - Società di servizi
   - Studi Medici associati
   - Ospedale, cliniche ed ASL
   - Forze armate

Il software permette di configurare gli accessi, i profili di autorizzazione e il trattamento dei dati sia come TITOLARE del trattamento, sia come RESPONSABILE del trattamento.

Le configurazioni proposte da GEA sono idonee a garantire la corretta applicazione del GDPR alla maggior parte delle imprese. Tuttavia, ogni Titolare del Trattamento è tenuto a verificare e modificare le configurazioni proposte per allinearle al proprio ciclo produttivo, all'articolazione dei ruoli in azienda, per integrare le misure organizzative stabilite e per renderle coerenti con le particolarità del trattamento, con le finalità e con le modalità definite dal singolo titolare. Per maggiori dettagli si vedano i punti seguenti.

A titolo esplicativo:
Es.1 Le limitazioni stabilite per l'RSPP possono essere rimosse qualora appartenga alla classe medica.
Es.2 Le limitazioni stabilite per l'RSPP possono essere aumentate qualora sia un soggetto esterno all'impresa.
Es.3 In caso di distacco del lavoratore, possono essere stabiliti nuovi privilegi d'accesso per il datore di lavoro distaccante.

Gea di Fioretti Massimiliano SAS & C.
Via dei Gemelli, 7 – 00040 Ardea (RM)
C.F. e P.I. 11101001003
Telefono 06.9179258
Fax 06.45501935
Email: info@gea-software.com

2. MODALITÀ DI FUNZIONAMENTO

Il software può essere acquistato ed usato in diverse modalità:

- Locale (computer singoli degli utenti)
- Server locali (LAN aziendale)
- Server Cloud (accessibile via internet, il server risiede fisicamente a Milano in una webfarm certificata ISO 27001)

La modalità in Server Cloud consente la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico

GEA, oltre ad aver sviluppato il software, eroga servizi di assistenza tecnica, formazione, hosting del sistema.

A seconda della tipologia di installazione e dei servizi richiesti, GEA assume il ruolo di AMMINISTRATORE DI SISTEMA o di RESPONSABILE DEL TRATTAMENTO, con formale lettera di nomina e applicazione delle previsioni contrattuali di cui all'art 28 comma 3 del GDPR.

In particolare, come Responsabile del Trattamento, GEA garantisce che:

- i dati personali siano trattati soltanto su istruzione documentata del titolare del trattamento;
- le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- siano adottate le misure di sicurezza previste all'art. 32 del GDPR
- non si ricorra ad un altro responsabile del trattamento senza preventiva notifica al titolare;
- si provveda ad agevolare ogni interessato che desideri esercitare i propri diritti, tra cui il diritto di accesso ai dati;
- si garantisca al titolare il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su scelta del titolare del trattamento, vengano cancellati o restituiti tutti i dati personali alla scadenza naturale del contratto e vengano cancellate le copie esistenti, salvo specifici obblighi di conservazione previsti dalla legge;
- vengano messe a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di legge;
- sia consentita qualsiasi attività di verifica al titolare del trattamento o ad un altro soggetto da questi incaricato.

Gea di Fioretti Massimiliano SAS & C.
Via dei Gemelli, 7 – 00040 Ardea (RM)
C.F. e P.I. 11101001003
Telefono 06.9179258
Fax 06.45501935
Email: info@gea-software.com

3. UTENTI – TITOLARI E/O RESPONSABILI DEL TRATTAMENTO:
   - Amministratore
   - Superuser
   - Medico coordinatore
   - Medico
   - Infermiere
   - RSPP
   - Amministrativo/Impiegato
   - Azienda

Il sistema prevede diverse funzioni di addetti al trattamento per consentire diversi livelli di accesso ai dati, con limitazioni di trattamento per i distinti utenti, in relazione alle istruzioni del Titolare ed alla natura dei dati stessi.

L'Amministratore di Sistema (GEA) potrà accedere ai dati solo per ragioni di carattere tecnico, finalizzate alla risoluzione di problemi, al mantenimento ed aggiornamento dell'applicazione; sono adottate misure di protezione tali da impedire a GEA l'accesso e la visibilità delle informazioni personali nel caso di accesso al sistema per ragioni tecniche.

Nel rispetto dei principi sopra descritti, le verifiche di funzionamento, qualora richiedano l'accesso ai database, qualora possibile, saranno condotte unicamente con set di dati di test completamente anonimi.

4. SICUREZZA/PROTEZIONE
   - PROFILI DI AUTENTICAZIONE: per l'assegnazione di un'utenza è obbligatorio inserire i dati identificativi della persona fisica.

   - PROFILI DI AUTORIZZAZIONE: il database fornisce un suo strato di sicurezza basato su account utente ai quali vengono associati i relativi permessi (ovvero la regolamentazione dell'accesso ai differenti dati ai soli utenti autorizzati).

   - REQUISITI DI COMPLESSITÀ DELLE PASSWORD: le password devono essere necessariamente costituite da minimo 8 caratteri alfanumerici, con caratteri maiuscoli, minuscoli e speciali (esempio: AfgKttu@18), con predisposto obbligo di modifica periodica configurabile, quale procedura imposta e utile a garantire una maggior efficacia nella protezione di accesso ai dati.

   - LOG: Tutte le attività effettuate direttamente dall'utente incaricato sono tracciate, a consentire valutazioni/verifiche di efficacia delle misure tecniche ed organizzative adottate ed il singolo utente può, nel caso, essere sempre bloccato dal Titolare del Trattamento, a mezzo dell'Amministratore di Sistema.

   - CRITTOGRAFIA: i dati viaggiano criptati e trasmessi nel protocollo https ed anche il database (Firebird all'attuale versione 2.5) è criptato. Sono adottate tecnologie di criptazione documentate e aggiornate rispetto a eventuali vulnerabilità. Non sono adottate tecnologie proprietarie o segrete.

Gea di Fioretti Massimiliano SAS & C.
Via dei Gemelli, 7 – 00040 Ardea (RM)
C.F. e P.I. 11101001003
Telefono 06.9179258
Fax 06.45501935
Email: info@gea-software.com

– ACCESSO E SICUREZZA DELLE INFRASTRUTTURE: in rispondenza al GDPR, sono adottate tutte le misure necessarie per preservare la sicurezza e la riservatezza dei dati personali trattati, in particolare per impedire che vengano violati, danneggiati o che soggetti terzi non autorizzati vi accedano - i dati archiviati con Urano4web in modalità Cloud restano di proprietà del cliente – Serverweb provvede alla conservazione fisica dei dati, ma non può accedere agli stessi.

– IL DATACENTER: è certificato, a garantire i migliori livelli di protezione e sicurezza dei dati, ovvero:
  - PVI – DSS: il Private Cloud è certificato PCI-DSS Livello 1 - Questa certificazione permette ai clienti Serverweb di usufruire di un'infrastruttura conforme agli standard PCI SSC (PCI Standard Security Council) per l'archiviazione ed il trattamento dei dati delle carte di pagamento
  - ISO/IEC 27001 (2013 per le soluzioni Cloud dedicato): questo standard attesta un'adeguata organizzazione della sicurezza
  - Attestazioni SOC 1 tipo II e SOC 2 tipo II: Il livello di sicurezza del Private Cloud è riconosciuto anche dalle attestazioni SOC 1 tipo II (SSAE 16 e ISAE 3402) e SOC 2 tipo II. Queste attestazioni internazionali garantiscono l'adeguatezza e l'efficacia dei controlli interni associati alla sicurezza del sistema informativo
  - Star self-assessment - Cloud Security Alliance: questa iniziativa informa i clienti ServerWeb relativamente alla conformità dei propri servizi di Cloud Computing alle best practice CSA e precisa le misure adottate per garantire la sicurezza del sistema informativo
  - Certificazione OpenStackpowered: il datacenter ha ricevuto la certificazone OpenStack nell'ottobre 2016

- RESILIENZA: ove, per ipotesi, si verificasse un eventuale violazione del sistema, questa sarebbe immediatamente segnalata e tracciata.

- AGGIORNAMENTO: il programma viene periodicamente aggiornato per garantire un costante miglioramento della sicurezza e delle prestazioni, l'immediata protezione da vulnerabilità, l'adeguamento delle funzionalità ad ogni esigenza

- SEPARAZIONE: i dati particolari sono separati dagli altri dati personali. Questa separazione, in particolare, è funzionale agli obblighi delle pubbliche amministrazioni o da queste specificamente richiesti ai loro responsabili del trattamento.

- NOTIFICA DATA BREACH: i dati sono pseudonimizzati e cifrati, con oscuramento delle informazioni, logica destrutturata ed inintelligibili. In caso di Data Breach, non è necessario dar corso alla Notifica della violazione agli interessati ai sensi dell'art. 34 del GDPR.

Gea di Fioretti Massimiliano SAS & C.
Via dei Gemelli, 7 – 00040 Ardea (RM)
C.F. e P.I. 11101001003
Telefono 06.9179258
Fax 06.45501935
Email: info@gea-software.com

5. REGISTRO DEL TRATTAMENTO:
   CARATTERISTICHE PRINCIPALI E STRUTTURA DEI DATI OGGETTO DEL TRATTAMENTO

- *Anagrafica – Aziende*: nell'area è possibile gestire i dati identificativi di ogni singola Azienda ed inoltre le Sedi, i Reparti, i Sopralluoghi ed i Corsi di Formazione. Nella finestra Azienda è possibile allegare ogni tipo di documentazione relativa all'azienda stessa, stampare direttamente il modello per la nomina del Medico Competente, il modello DDL (dati occupazionali forniti dal Datore di lavoro ai sensi del D.Lgs. 81/2008 Allegato 3A) da inviare al Datore di lavoro e generare un report relativo ai protocolli, con i rischi, presenti nell'azienda stessa.
- *Anagrafica – Dipendenti*: nell'area è possibile gestire i dati identificativi di ogni singolo dipendente dell'azienda selezionata. Tutti i dati richiesti per la compilazione della Cartella Sanitaria e di Rischio ai sensi del D.Lgs 81/2008 Allegato 3A, quali: dati identificativi, domicilio, medico curante, ruolo del dipendente, assenze, D.P.I., corsi di formazione, rischi ed eventuali esami complementari. E' inoltre possibile allegare ogni tipo di documentazione relativa al dipendente stesso e una foto tessera.
- *Sanità*: nell'area è possibile gestire i dati delle visite, gli accertamenti e l'anamnesi lavorativa, gli infortuni, le malattie professionali, le invalidità, le vaccinazioni ed i giudizi di idoneità; cioè tutti i dati necessari alla compilazione della Cartella Sanitaria e di rischio ai sensi del D.Lgs. 81/2008 Allegato 3A del dipendente selezionato. La Cartella Sanitaria così compilata può essere stampata in vari formati da Word a Pdf (Le stampe in Urano4Web sono circa 110 tutte personalizzabili dall'utente grazie ad un designer che consente di inserire loghi di società, immagini, cambiare il carattere, il colore ed altro). Nella cartella Accertamenti è anche possibile inserire da scanner o digitale, e salvare, tracciati di ECG o radiografie ed allegarli al relativo accertamento.
- *Protocollo Sanitario*: nell'area è possibile gestire i Protocolli, i Rischi e gli Accertamenti e pertanto non sono trattati dati personali. Il bottone Protocolli consente di creare il protocollo sanitario con estrema semplicità e velocità. Dopo aver inserito la descrizione prescelta sarà sufficiente selezionare i rischi e gli accertamenti. Urano4Web fornisce un elenco generale di rischi ed accertamenti, in ogni momento modificabile dall'utente.
- *Organizer – Agenda*: l'area fornisce strumenti utili come la Rubrica e l'Agenda, con dati identificativi/anagrafici. L'Agenda consente di visualizzare e pianificare lo scadenziario delle visite, avendo così la possibilità di conoscere in ogni momento in quali aziende, entro una certa data, il medico dovrà svolgere le visite, dei sopralluoghi, delle vaccinazioni, dei corsi, degli eventi e degli infortuni. E' anche possibile decidere quanto tempo prima Urano4Web dovrà avvertire l'utente dei propri appuntamenti. In agenda è anche possibile visualizzare e stampare un elenco della mail inviate all'azienda.
- *Condivisione*: Urano4Web permette di condividere in automatico il Giudizio di Idoneità con il lavoratore e con il datore di lavoro. Urano4Web permette di condividere in automatico la Cartella con il lavoratore.
- *Informativa*: è prevista l'informativa per il lavoratore, in forma cartacea o in formato elettronico, con modello che riporta informazioni concise, trasparenti, intellegibili e conformi all'art. 13 del GDPR
- *Firma*: tutta la documentazione elettronica è corredata di firma grafometrica protetta e certificata ISO 27001.

Gea di Fioretti Massimiliano SAS & C.
Via dei Gemelli, 7 – 00040 Ardea (RM)
C.F. e P.I. 11101001003
Telefono 06.9179258
Fax 06.45501935
Email: info@gea-software.com

- *Statistiche*: l'area consente una facile estrapolazione dei dati, l'utente ha la possibilità di effettuare statistiche per ogni area del programma, visualizzabili con dei grafici, consente inoltre di creare e stampare la RELAZIONE SANITARIA di fine anno ai sensi del D.Lgs. 81/2008 e l'Allegato 3B, art. 40.
- *Contabilità*: l'area fornisce la possibilità di creare i listini prezzi di ogni singolo accertamento per azienda, di gestire costi fissi o di calcolare sconti, per poi procedere alla fatturazione. E', infatti possibile, creare e stampare fatture da inviare all'azienda.
- *Utility*: l'area fornisce la Gestione tabelle ed i Parametri del programma. Nella finestra Carica Dati dei Parametri è possibile, tramite un file fornito dalla Gea, caricare con un semplice click l'anagrafica dell'azienda con i relativi dipendenti direttamente in Urano4Web, bypassando l'iniziale inserimento manuale, sarà infatti sufficiente inviare il file all'Ufficio del Personale dell'azienda presa in carico, fare compilare i campi per poi procedere al caricamento in Urano4Web. La Gestione tabelle fornisce la possibilità di modificare o ampliare i dati relativi agli Accertamenti, ai Rischi, ai Medici ed alle Città.

GDPR – REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI 2016/679

GEA conosce molto bene il mondo della medicina del lavoro e sa fare il software. Per questa ragione, per poter garantire la massima protezione dei dati personali e l'esatto adempimento degli obblighi relativi al GDPR, ci siamo fatti affiancare da un Team di specialisti che, da oltre 20 anni, si dedica alla consulenza legale e tecnologica in materia di privacy. Il Team è diretto da Avv. M. Chiocchi e Dott. C. Bernieri, specialisti certificati ANORC e IAPP.

Il software Urano4Web, la documentazione a corredo del programma, le configurazioni proposte del sistema, i moduli di informativa, la qualifica dei su-processor (sub responsabili del trattamento) e dei provider di servizi tecnici accessori sono stati oggetto di analisi, valutazione e messa a norma. Urano4Web è costantemente allineato all'evoluzione della normativa e integra in modo dinamico tutti i provvedimenti e le linee guida del Garante Privacy e del WP29.

Gea di Fioretti Massimiliano SAS. & C

Massimiliano Fioretti