PRIVACY POLICY

Our GDPR Compliance Statement

Welcome to TESISQUARE®

CONNECTING PEOPLE, TECHNOLOGY,
AND PROCESSES IN A COLLABORATION SQUARE

Revisione e approvazione

AZIONE	FUNZIONE	NOME	DATA
Approvato	Marco Cuniberti	DPO	21/03/2024
Verificato	Alessandro Cassinelli	Legal Manager	21/03/2024
Redatto	Francesca Bordino	Privacy Specialist	21/03/2024

Distribuzione

Ente / Ufficio	Funzione
Everyone	Everyone

Aggiornamento

VER	AUTORE	DATA	NOTE
1.0	Francesca Bordino	21/03/2024	Creazione Documento
2.0	Francesca Bordino	18/06/2024	Creazione paragrafo Policy di trasferimento dei dati extra UE

Sommario

1 Premessa

Il Regolamento Generale sulla Protezione dei Dati (GDPR), entrato in vigore nei paesi dell'Unione Europea il 25 maggio 2018, stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. Inoltre, protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali (art. 1 Regolamento UE 2016/679).

Il Regolamento si applica a tutte le imprese stabilite nei paesi dell'Unione Europea e ciò anche se gli interessati si trovano al di fuori dell'Unione.

Il Regolamento europeo non definisce in maniera analitica e predefinita gli adempimenti, lasciando alle imprese ampia autonomia nell'attuazione dei propri programmi di compliance.

2 Il nostro impegno

TESISQUARE si impegna a garantire l'applicabilità del Regolamento UE 2016/679, nelle forme e nei modi definite dall'azienda. A tal fine, TESISQUARE pone in essere strumenti e misure di protezione dei dati utili a garantire la massima e costante conformità al GDPR.

3 Misure organizzative per garantire la compliance al GDPR

TESISQUARE adotta misure organizzative interne necessarie per il rispetto delle disposizioni normative vigenti in materia di tutela e protezione dei dati personali. Le misure sottoindicate vengono adottate dall'organizzazione nel rispetto dei principi generali della protezione dei dati (trasparenza, finalità, minimizzazione dei dati, limitazione nel tempo della durata del trattamento, conservazione della integrità dei dati).

Formazione periodica di tutti i dipendenti
TESISQUARE attiva video-corsi di formazione sul GDPR attivati per tutti i dipendenti in modalità e-learning e corsi di approfondimento in ambito privacy, mirati per specifiche mansioni aziendali.

Organigramma privacy
Per il raggiungimento degli obiettivi privacy interni all'organizzazione, TESISQUARE si dota di un organigramma di funzioni, definito attraverso l'attribuzione di ben determinati compiti e delle relative responsabilità a tutte le figure, interne ed esterne all'organizzazione, che concorrono a sviluppare i processi aziendali in cui vengono gestiti i dati personali.

Nomina di referenti interni
TESISQUARE designa i referenti coordinatori in tema di privacy e data protection in ottemperanza al principio di accountability del Titolare e relativi compiti, ai sensi del GDPR. Limitatamente agli ambiti dei trattamenti individuati per ciascun referente interno,

TESISQUARE riconosce al referente designato il potere di firmare per suo conto le lettere di nomina del Responsabile Esterno del Trattamento qualora ne ravvisi la necessità nei confronti del Cliente/Titolare del trattamento. Inoltre, il soggetto designato tramite l'atto di nomina, ha il dovere di compiere tutto quanto è necessario per il rispetto delle disposizioni normative vigenti in materia di tutela e protezione dei dati personali.

Lettere di incarico a ciascun dipendente in relazione alla mansione svolta

TESISQUARE procede alla designazione dei soggetti autorizzati al trattamento dei dati personali ai sensi del Regolamento Europeo 2016/679 e relativi compiti. In particolare, si autorizzano i dipendenti al trattamento di dati personali, così come censiti nel Registro dei Trattamenti.

Nomina e verifica dell'operato degli Amministratori di Sistema

TESISQUARE mantiene un elenco aggiornato degli Amministratori di Sistema ("ADS") e adempie alle prescrizioni indicate nel Provvedimento Garante Privacy 27 novembre 2008. In particolare, TESISQUARE procede alla designazione delle figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché amministratori di basi di dati, di reti, di apparati di sicurezza, di sistemi software complessi e che nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati. TESISQUARE procede inoltre, con cadenza almeno annuale, a verificare l'operato degli ADS.

Sottoscrizione, da parte di ciascun dipendente, di un accordo di riservatezza all'atto dell'assunzione

All'atto dell'assunzione TESISQUARE sottoscrive con i propri dipendenti un accordo avente per oggetto gli obblighi di riservatezza e segretezza in ordine alle informazioni riservate di cui lo stesso dipendente sia venuto a conoscenza in conseguenza o per effetto del rapporto di lavoro, ritenendosi tali tutte le informazioni, i dati e i documenti di carattere confidenziale, ovvero oggetto di segreto industriale, di proprietà di TESISQUARE ovvero di sue consociate o controllate, nonché ogni altra informazione di qualsiasi natura appresa dai clienti di TESISQUARE.

Tenuta dei registri del titolare o del responsabile

Ai sensi dell'art. 30 GDPR, TESISQUARE tiene un registro del titolare e responsabile aggiornato costantemente sulla base di attività di trattamento effettivamente svolte. La redazione del registro del trattamento è funzionale al rispetto del principio di responsabilizzazione; al rispetto degli adempimenti in materia di sicurezza; alla programmazione delle modalità di riscontro all'esercizio dei diritti degli interessati.
I registri contengono in particolare, il nome del titolare del trattamento; la descrizione delle categorie di interessati; la descrizione delle categorie di dati personali; una descrizione generale delle misure di sicurezza.

Policy e procedure in ambito privacy

TESISQUARE si è dotata di un robusto impianto di procedure e di policy relative al trattamento dei dati personali che svolge sia in qualità di Titolare, sia in qualità di Responsabile. Tali policy

sono discusse e approvate dal Privacy team interno, dal Comitato Privacy, dal Data Protection Officer e dalle altre figure ed enti aziendali eventualmente impattati.

Riunioni periodiche di un Comitato Privacy interno
TESISQUARE si è dotata di un Comitato Privacy interno a cui prendono parte le figure aziendali maggiormente coinvolte sul tema e il DPO, per allineamento e discussione su temi trasversali.

Nomina di un DPO
TESISQUARE ha provveduto alla designazione di un responsabile della protezione dei dati (DPO) contattabile all'indirizzo mail: dpo@tesisquare.com.

Valutazioni di impatto continue (privacy by design)
Ai sensi degli articoli 35 e 36 del GDPR e sulla base del documento WP248 - Linee guida sulla valutazione di impatto nella protezione dei dati adottato dal Gruppo di lavoro ai sensi dell'art. 29, TESISQUARE ha predisposto una propria metodologia per l'analisi e la valutazione dei trattamenti che, considerata la natura, l'oggetto, il contesto e la finalità del trattamento, presentano un rischio elevato per i diritti e le libertà delle persone fisiche al fine di procedere al valutazione dell'impatto sulla protezione dei dati personali prima di iniziare il trattamento.

Audit di terza parte periodici
TESISQUARE organizza con cadenza almeno annuale azioni sorveglianza da parte di figure audit esterne, al fine di rilevare osservazioni/punti di attenzione/non conformità che consentono all'organizzazione di operare puntualmente per affinare e rafforzare alcuni aspetti che sono vitali ai fini del recepimento completo del GDPR e delle normative che disciplinano gli aspetti di data protection.

Informative
L'azienda predispone, in ottemperanza all'art. 13 e 14 GDPR, informative agli interessati per fornire indicazioni sulle finalità e modalità dei trattamenti, laddove ne vengono raccolti i dati. Tali trattamenti sono improntati ai principi di correttezza, liceità, trasparenza e di tutela della riservatezza e dei diritti dei soggetti interessati.

Le principali informative predisposte sono:

1. Informativa privacy per i candidati
2. Informativa privacy per i clienti
3. Informativa privacy per i fornitori
4. Informativa privacy per sito internet Tesisquare
5. Informativa privacy Whistleblowing
6. Informativa Marketing

Altre informative vengono di volta in volta predisposte qualora l'azienda intraprenda un nuovo trattamento di dati personali in qualità di Titolare.

Certificazione ISO 27001
TESISQUARE è certificata UNI CEI EN ISO/IEC 27001:2017 e mantiene un Sistema di Gestione della Sicurezza delle Informazioni (ISMS) certificato da audit di terza parte periodici.

4 Misure tecniche per garantire la compliance al GDPR

TESISQUARE mantiene un programma misure tecniche progettate per proteggere i dati propri e dei Clienti da perdita, accesso o divulgazione accidentale o illegale, nonché volte a identificare i rischi interni ragionevolmente prevedibili per la sicurezza e l'accesso non autorizzato alla rete e ridurre al minimo i rischi per la sicurezza.

Autorizzazione logica di accesso
TESISQUARE definisce i profili di accesso nel rispetto del privilegio minimo necessario per l'esecuzione dei compiti assegnati. I profili di autorizzazione sono individuati e configurati prima dell'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari allo svolgimento delle operazioni di trattamento.
Tali profili sono soggetti a verifiche periodiche volte a verificare la sussistenza delle condizioni per la conservazione dei profili assegnati.

Incident Management
TESISQUARE ha implementato una specifica procedura di Incident Management al fine di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile, garantendo il mantenimento dei migliori livelli di servizio.

Data Breach
TESISQUARE ha implementato una specifica procedura volta alla gestione di eventi e incidenti con potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento delle incidente/violazione nonché le modalità attraverso le quali comunicare al Cliente violazioni dei dati personali.

Protezione dai malware
I sistemi sono protetti dal rischio di intrusione e di azione del programma mediante l'attivazione di idonei strumenti elettronici aggiornati regolarmente.

Credenziali di autenticazione
I sistemi sono configurati in modo idoneo per consentire l'accesso solo a soggetti in possesso di credenziali di autenticazione che ne consentano l'identificazione univoca. Tra questi, codice associato ad una password, riservata e conosciuta solo dalla stessa; dispositivo di autenticazione di proprietà e ad uso esclusivo dell'utente, dove l'accesso è consentito solo con un codice identificativo e una password.

Password
Per quanto riguarda le caratteristiche di base ovvero l'obbligo di modifica al primo accesso, lunghezza minima, assenza di elementi facilmente riconducibili alla materia, regole di complessità, scadenza, storia, valutazione contestuale di robustezza, visualizzazione e archiviazione, il password è gestita secondo le migliori pratiche. Ai soggetti cui sono attribuite

le credenziali sono impartite istruzioni in merito alle modalità da adottare per garantire il segreto.

Logging
I sistemi sono configurati in modo da consentire il tracciamento degli accessi e, ove opportuno, delle attività svolte dalle diverse tipologie di utenti (amministratore, super utente, ecc.) protetti da adeguate misure di sicurezza che ne garantiscano l'integrità.

Backup & restore
Sono adottate misure idonee a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi compatibili con i diritti degli interessati.

Vulnerability Assessment & Penetration Test
TESISQUARE, per il tramite terze parti, svolge periodicamente attività di analisi di vulnerabilità volte a rilevare lo stato di esposizione a vulnerabilità note, sia in relazione ad ambiti infrastrutturali che applicativi.
Ove ritenuto opportuno in relazione ai potenziali rischi individuati, tali controlli sono periodicamente integrati con specifiche azioni di Penetration Test, attraverso simulazioni di intrusione utilizzando diversi scenari di attacco, con l'obiettivo di verificare il livello di sicurezza di applicazioni/sistemi/reti attraverso attività che mirano a sfruttare le vulnerabilità rilevate per aggirare i meccanismi di sicurezza fisica/logica e accedervi.
Gli esiti delle verifiche vengono tempestivamente e nel dettaglio esaminati per individuare e mettere in atto i punti di miglioramento necessari a garantire l'elevato livello di sicurezza richiesto.

Firewall
I dati personali sono protetti dal rischio di intrusione attraverso firewall di nuova generazione tenuti aggiornati in relazione alle migliori tecnologie disponibili.

Sicurezza sulle linee di comunicazione
I provider dei servizi di hosting selezionati da TESISQUARE sono dotati di protocolli di comunicazione sicuri in linea con quanto la tecnologia mette a disposizione.

Sicurezza della rete
TESISQUARE manterrà i controlli di accesso e le politiche per gestire quale accesso è consentito alla rete da ogni connessione di rete e utente, compreso l'uso di firewall o tecnologie funzionalmente equivalenti e controlli di autenticazione.
TESISQUARE manterrà piani di azioni correttive e di risposta agli incidenti per rispondere a potenziali minacce alla sicurezza.

5 Misure fisiche per garantire la compliance al GDPR

Controlli di accesso fisico

I componenti fisici delle soluzioni software TESISQUARE sono alloggiati in strutture anonime (le "Strutture"). I controlli fisici delle barriere sono utilizzati per impedire l'ingresso non autorizzato alle Strutture sia al perimetro che ai punti di accesso degli edifici.

Il passaggio attraverso le barriere fisiche presso le Strutture richiede la convalida elettronica del controllo degli accessi (es. sistemi di accesso alle carte, ecc.) o la convalida da parte del personale di sicurezza umano (es. servizio di guardia giurata a contratto o interno, receptionist, ecc.).

Ai dipendenti e agli appaltatori vengono assegnati badge identificativi con foto che devono essere indossati mentre i dipendenti e gli appaltatori si trovano in una qualsiasi delle strutture.

I visitatori sono tenuti a registrarsi con il personale designato, devono esibire un'identificazione adeguata, gli viene

assegnato un badge identificativo del visitatore che deve essere indossato mentre il visitatore si trova in una qualsiasi delle strutture

e sono continuamente scortati da dipendenti o appaltatori autorizzati durante la visita alle strutture.

Accesso limitato di dipendenti e appaltatori

TESISQUARE fornisce l'accesso alle Strutture a quei dipendenti e appaltatori che hanno una legittima esigenza commerciale di tali privilegi di accesso.

Quando un dipendente o appaltatore non ha più la necessità aziendale dei privilegi di accesso a lui assegnati, i privilegi di accesso vengono tempestivamente revocati.

Protezioni di sicurezza fisica

Tutti i punti di accesso (diversi dalle porte d'ingresso principali) sono mantenuti in uno stato protetto (bloccato). I punti di accesso alle Strutture sono monitorati da telecamere di videosorveglianza atte a registrare tutte le persone che accedono alle Strutture.

TESISQUARE mantiene inoltre sistemi elettronici di rilevamento delle intrusioni atti a rilevare accessi non autorizzati alle Strutture, compreso il monitoraggio dei punti di vulnerabilità (es. porte di ingresso primarie, porte di uscita di emergenza, botole da tetto, porte di banchina, ecc.) con contatti porta, dispositivi di rottura vetri , rilevamento del movimento interno o altri dispositivi progettati per rilevare le persone che tentano di accedere alle Strutture.

6 Policy di trasferimento dei dati

TESISQUARE conserva e tratta i dati dei clienti unicamente in data center europei.

TESISQUARE non esclude che il trattamento dei dati dei clienti possa avvenire da altre società che risiedono nell'Unione Europea o da altre legal entity extre UE.

Laddove verranno individuati data center diversi da quelli ad oggi presenti in Europa per la conservazione e il trattamento dei dati dei clienti, sarà premura di TESISQUARE adottare le misure di sicurezza previste dal GDPR o altre misure di sicurezza rafforzate.