Autore	Ufficio privacy
Approvazione	Lorenzo Ciuffi

Versione Revisione

Versione	Autore	Consultazione DPO	Data emissione	Motivo della revisione
0.0	Ufficio Privacy	17/10/2019	18/10/2019	Prima emissione – versione servizio CLOUD (non gestito)
1.0	Ufficio Privacy	01/01/2020	01/01/2021	Modificato legale rappresentante
2.0	Ufficio Privacy	15/04/2021	16/04/2021	Modificati i tempi di retention

PARERE DPO
Ok

SERVIZI & PRODOTTI TPC&JOIN

RESPONSABILE DEL TRATTAMENTO					
Denominazione	TPC&Join S.r.l.				
Partita Iva	02114690486				
Indirizzo	Viale Eleonora Duse, 12				
Città	Firenze	Cap	50137	PV	FI
Legale Rappresentante	Lorenzo Ciuffi				

STRUTTURA ORGANIZZATIVA			
Divisione	Divisione TPC	Responsabile Divisione	Lorenzo Ciuffi

INCARICATI DEL TRATTAMENTO
Addetti analisi, sviluppo, controllo qualità, help desk, consulenti applicativi, sistemisti

DATI DI CONTATTO			
Titolare del trattamento	TPC&Join	gdpr@tpc.it	055601090
Rappresentante del titolare			
Responsabile protezione dati (DPO)	Mario Brocca	gdpr@tpc.it	055601090

DESCRIZIONE
TPC ha sviluppato soluzioni software su varie piattaforme che hanno come obiettivo la gestione dei dati anagrafici e retributivi delle Risorse Umane dei propri clienti. L'accesso a tali informazioni avviene tramite profilazione degli utenti e gestione delle relative credenziali. Si rimanda alle sezioni successive per il dettaglio tecnico di ogni specifica piattaforma.

FINALITA' DEL TRATTAMENTO

Gestione dei dati personali di interessati e aziende finalizzato alla gestione dei dati personali nei singoli applicativi utilizzati per gestire i singoli adempimenti di gestione amministrativa e contabile del personale.

CATEGORIA INTERESSATI

Dipendenti, apprendisti, tirocinanti, stagisti, collaboratori, fornitori, appaltatori e visitatori.

CATEGORIE DI DATI PERSONALI

Dati anagrafici di personale dipendente, apprendisti, tirocinanti, stagisti, collaboratori, fornitori, appaltatori e visitatori in funzione dell'applicativo che li utilizza.
Dati relativi al rapporto di lavoro ed economici.
Ci sono dati non identificabili che sono salvati su archivi di tipo gerarchico attraverso estrazioni che derivano dai singoli applicativi.
Negli archivi ci possono essere i seguenti dati che presentano rischi specifici:

- iscrizione a sindacato
- valutazione professionale di dipendenti e collaboratori
- minori e stato di famiglia
- dati relativi alla salute
- situazione economica

I prodotti TPC sono suddivisi in tre aree principali in base all'architettura di sviluppo (da parte di TPC) e di utilizzo (da parte dei clienti):

<u>Area IBM System i (AS/400)</u>

- GIP – Gestione Integrata Presenze
- BIP – Budget Integrato del Personale
- GNS – Gestione Nota Spese e Trasferte
- UNL – Unificato LAV
- CML – Certificati Medici onLine
- BON – Bonifici Aziendali
- CUT – Certificazione Unica TPC

<u>Area IBM Lotus Domino / Notes</u>

- Candidati
- Risorse (Anagrafica, Documenti, Formazione, Scadenzario, Retribuzioni)
- Organizzazione (Job Position, Mansioni, Attività, Competenze, Requisiti)
- Comunicazioni (Workflow ferie e permessi, Bacheca)
- Valutazioni (Valutazione Competenze)
- Visite Mediche
- Provvedimenti disciplinari

<u>Area Web</u>

- Presenze Web – Workflow – Certificati medici
- Generatore Documenti
- Gestione Ticket
- Gestione Scenari di Budget
- MBO – Sistema Premiante

CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI
Subappaltatori Business Partner TPC Incaricati di attività di assistenza e manutenzione
TRASFERIMENTO DATI ALL'ESTERO
No
TEMPI DI RETENTION
I termini devono essere definiti dal Cliente e l'attività di cancellazione dovrà avvenire manualmente o definita col fornitore a livello progettuale.

DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

1. MISURE DI SICUREZZA IMPLEMENTATE NEI SOFTWARE

I prodotti TPC sono suddivisi in tre aree principali in base all'architettura di sviluppo (da parte di TPC) e di utilizzo (da parte dei clienti). Il software raccoglie solo i dati necessari rispetto alla finalità con cui è stato concepito.

Le principali misure di sicurezza sono demandate all'architettura del sistema, comune a tutte le piattaforme:

- *Gestione credenziali di accesso:*

- Username: l'accesso al sistema avviene solo attraverso l'identificazione univoca del soggetto che vi accede. Nel sistema c'è una credenziale amministrativa che viene consegnata al titolare e da questo utilizzabile solo in circostanze eccezionali. Il titolare deve predisporre una procedura organizzativa affinché tale utenza sia assegnata ad un unico incaricato e sia gestita in conformità alle buone regole di gestione.
- Password: le regole di complessità della password sono configurabili nel sistema da parte del titolare. Potrà scegliere diversi gradi di complessità e applicarli a tutti gli utenti del sistema. Sono configurabili anche i tempi di sostituzione delle password.
- Criteri di complessità per le impostazioni delle credenziali: le credenziali di accesso possono essere impostate secondo diversi criteri di complessità dal Titolare.
- Il Cliente ha la possibilità di impostare la funzione di blocco account a tempo oppure il blocco account per superamento tentativi di login fail. Inoltre, c'è la possibilità di impostare un numero massimo di tentativi di accesso e un numero massimo di cambi password in un giorno
- Solo per il prodotto Presenze Web è possibile implementare un sistema di autenticazione integrata basata su Active Directory.

- *Minimizzazione*

- Profili di autorizzazione: il Titolare può configurare l'accesso ai dati personali trattati nel sistema a seconda delle attività svolte dagli utenti.
- In alcuni archivi è prevista l'identificazione di chi ha trattato i dati
- Strumenti di log: attraverso i log del server è possibile verificare gli accessi degli utenti al sistema
- Se correttamente impostate dal cliente è possibile generare utenze di servizio individuali per il personale di assistenza. Coloro che eseguono assistenza e manutenzione sulla procedura hanno utenze nominali che potranno essere attivate e disattivate dal Titolare in funzione della necessità

- *Tecniche di crittografia:*

I prodotti TPC sfruttano le funzioni di crittografia disponibili nelle rispettive piattaforme di appartenenza.

- *Privacy by default*

- I prodotti TPC utilizzano le funzioni native della piattaforma su cui sono basati. Il sistema di default non attribuisce all'utente autorizzazioni. Sarà il Titolare in autonomia a scegliere la profilazione utente idonea

e ad attribuire le autorizzazioni in funzione dell'area omogenea di cui fa parte l'utente o del profilo di autorizzazione individuale.

- Nel sistema Lotus/Domino e per i prodotti web quando viene generato un nuovo utente questo non ha accesso ad alcuna informazione
- Nel sistema AS/400 quando viene generato un nuovo utente questo ha accesso ha tutte le informazioni e quindi occorre intervenire sul Modulo Base ACG per limitare le funzioni a menù e sulla riservatezza applicativa per limitare l'accesso ai dati.
  - *Diritti degli interessati*
- Per garantire agli interessati il diritto all'oblio, è sufficiente che inviino una richiesta al Titolare che farà le opportune valutazioni. Qualora il Titolare decida che i dati debbano essere cancellati, potrà agire direttamente sul prodotto, cancellando i dati del dipendente all'interno di ogni applicativo.
- I dati raccolti sono trattati ai fini di elaborazioni amministrative contabili dei rapporti con il personale.
- L'applicativo consente l'estrazione di dati specifici riguardanti le singole sezioni e i singoli adempimenti. Le estrazioni possono esser fatte in CSV, Excel o in altre funzioni relative al sistema.
- Il Cliente può, previa analisi a livello progettuale, richiedere una valutazione di fattibilità di anonimizzatine dei dati.

Queste misure di sicurezza devono essere correttamente impostate da parte del Titolare.

2. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI DI ASSISTENZA

ASSISTENZA ON SITE

Gli addetti TPC&Join accedono presso la struttura del cliente per fare formazione o effettuare attività tecnica di manutenzione.
In questo caso gli addetti TPC&Join lavorano come se facessero parte della struttura del cliente e adottano tutte le procedure che il cliente ritiene opportune. I clienti potranno generare utenze individuali per l'accesso ai loro sistemi, oppure potranno far accedere in affiancamento per formare il loro personale.
Qualora durante l'attività di assistenza l'addetto TPC&Join abbia la necessità di prelevare archivi o db di cui necessita per risolvere le problematiche evidenziate è necessario che informi il cliente e lo registri inviandogli una email.
Qualora vi fosse la necessità di conservare gli archivi per il tempo necessario al collaudo della soluzione adottata, dovrà essere informato il cliente sul tempo massimo di conservazione di tali archivi.

ASSISTENZA TELEFONICA / TICKETS

Non presenta problemi da un punto di vista di trattamento di dati personali. Non sono trasmessi dati o archivi e la comunicazione rimane verbale.

ASSISTENZA TRAMITE EMAIL / TICKETS

TPC ha introdotto nuove policy per l'assistenza tramite Help Desk, per evitare che le credenziali di accesso ai sistemi dei clienti siano fornite tramite e-mail.
Anche nel caso in cui il cliente invii per sua iniziativa tali credenziali, i tecnici TPC&Join non faranno uso di tali credenziali e informeranno il cliente che questa modalità viola il GDPR. Quindi verranno richieste credenziali individuali, oppure un collegamento con Team Viewer.
Infine, la messaggistica che intercorre tra l'operatore e il cliente è sempre riconducibile ad una risorsa TPC&Join.

ASSISTENZA ATTRAVERSO LA RICEZIONE DI DATA BASE DEI CLIENTI

Qualora per risolvere il problema segnalato dal cliente fosse necessario farsi mandare la base dati o altri file o query contenenti dati personali è necessario comunicare al cliente l'area ftp su cui dovrà caricare i file.

Area FTP

L'area FTP, assegnata univocamente ad ogni cliente, è impostata affinché possa essere effettuato solo l'upload e la cancellazione di quanto inviato dal cliente medesimo.
I file inviati risiederanno nell'area FTP per 72 ore, successivamente una routine cancellerà i file.

Scaricamento archivi tramite wetransfer o link di collegamento su ambienti clienti
In questo caso la gestione è in carico al cliente che ci fornisce le credenziali per accedere all'ambiente dove risiedono gli archivi.
L'assistenza dovrà scaricarli in dischi di rete non soggetti a backup e cancellarli al termine dell'attività come nelle altre ipotesi.

In ogni caso, al termine dell'attività presso gli uffici TPC&Join, il cliente sarà informato tramite email della cancellazione dell'archivio.

ASSISTENZA ATTRAVERSO COLLEGAMENTO DA REMOTO TEAM VIEWER

Questa modalità di collegamento sugli strumenti dei clienti garantisce la privacy in quanto:

- Il collegamento è sempre richiesto dal cliente
- Le credenziali di accesso sono sempre individuali
- Il cliente fa accedere i tecnici TPC&Join ad un ambiente con profilo di autorizzazione da lui scelto per far eseguire le attività di assistenza
- Il cliente può sconnettere il tecnico quando desidera

Attraverso Team Viewer è possibile far accedere anche l'assistenza di 2° livello alla stessa sessione aperta. In questo caso il cliente ne ha l'evidenza perché fornita dallo strumento e quindi accetta implicitamente tale modalità.
È essenziale utilizzare il Team Viewer TPC&Join in quanto licenziato e personalizzato con tutta la documentazione che deve essere prodotta dalla legge sul trattamento dei dati personali.
Solo in casi eccezionali e dopo attenta valutazione del responsabile e dell'ufficio privacy è possibile utilizzare altri strumenti di connessione che si comportano in modo uguale.
Si consiglia al cliente di creare comunque credenziali di accesso individuale per accedere alla propria infrastruttura.

ASSISTENZA ATTRAVERSO COLLEGAMENTO DA REMOTO SU IP PUBBLICI OPPURE TRAMITE VPN

Qualora l'attività di assistenza debba essere svolta su sistemi con IP pubblici, oppure tramite VPN o accessi privati è necessario che gli addetti TPC&Join entrino nei sistemi dei clienti:

- Previa autorizzazione del cliente
- Che abbiano ricevuto le credenziali individuali e le stesse siano attive per il tempo necessario all'esecuzione delle attività richieste
- Che al termine dell'attività siano disattivate

Le regole che riguardano gli ambienti dei clienti, in qualsiasi forma di delivery sono di seguito elencate:

- Per effettuare tutte le attività di assistenza e manutenzione sull'ambiente cliente è necessario che venga appositamente creata un'utenza all'interno del sistema come di seguito indicato:
- TPC + prime 3 lettere del cognome + prime 3 lettere del nome
- nella descrizione (nome completo) apporre: Utente TPC
- In questo modo il Cliente potrà riconoscere la provenienza dell'utenza stessa.
- Es: per il soggetto Rossi Mario dovrà essere creata l'utenza: TPCROSMAR
- Per la creazione dell'utenza dovrà essere coinvolto il cliente, condividendo con lui i diritti che verranno assegnati a quest'ultima