Active Trees Governance

Registro del trattamento del servizio

Versione n. 0 del 03/10/2024

RESPONSABILE DEL TRATTAMENTO					
Denominazione	Bookmark S.r.l.				
Partita Iva	03211600402				
Indirizzo	Via Eugenio Bertini, n. 247				
Città	Forlì	**Cap**	47122	**PV**	FC
Legale Rappresentante	Luigi Zirpoli				

STRUTTURA ORGANIZZATIVA			
Unità organizzativa	Team di prodotto - Active Trees ESG Zucchetti	**Responsabile UO**	Zirpoli Luigi

INCARICATI DEL TRATTAMENTO
Analisti, sviluppatori, addetti al controllo qualità, addetti help desk, consulenti applicativi e sistemisti

DATI DI CONTATTO			
Responsabile del trattamento	Bookmark S.r.l.	dpo@bkm.it	0543.777382
Rappresentante del titolare	N/A	N/A	N/A
Responsabile protezione dati (DPO)	Mario Brocca	dpo@zucchetti.it	0371.5943191

DESCRIZIONE
Software per la gestione degli obiettivi strategici, della struttura organizzativa, dei processi, dei progetti e dello sviluppo delle risorse umane.

FINALITA' DEL TRATTAMENTO
Gestione dei dati personali di interessati e aziende Titolari finalizzato alla gestione dei processi relativi alla governance aziendale. La finalità del trattamento è quella di erogare i servizi di assistenza e manutenzione al Titolare.

CATEGORIA INTERESSATI
Dipendenti e collaboratori del titolare.

CATEGORIE DI DATI PERSONALI
Dati anagrafici, indirizzi e-mail

CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI
Data center (Azure e AWS)
TRASFERIMENTO DATI ALL'ESTERO
No
TERMINI PER LA CANCELLAZIONE DEI DATI
Al momento della scadenza o della risoluzione del contratto e/o del servizio di riferimento, verranno cancellati in modo sicuro tutti i Dati personali del Cliente in nostro possesso entro 30 giorni, nella misura necessaria ai sensi della Legislazione applicabile in materia di protezione dei dati personali. Al termine della scadenza o della risoluzione del contratto, in occasione della cancellazione dei dati, una copia degli stessi sarà conservata per 12 mesi sul Cloud AWS, nei datacenter eu-central-1 (Francoforte) e l'unico trattamento degli stessi sarà la conservazione.
BACKUP
Il Backup avviene con la tecnologia fornita da Microsoft Azure Backup (per informazioni vedere https://learn.microsoft.com/it-it/azure/backup) I backup risiedono nel Cloud Azure di Microsoft, nei datacenter West Europe (Amsterdam) e NORTH Europe (Dublin). Il backup avviene per tutti i dati dell'applicativo, la retention viene indicata nei contratti. La cancellazione dei backup è governata dalla tecnologia di riferimento ed avviene sulla base della retention.
LOG
Le registrazioni degli accessi sono conservate per un anno e risiedono sul Cloud AWS, nei datacenter eu-central-1 (Francoforte). I logs sono conservati in maniera immodificabile e vengono cancellati autonomamente alla scadenza.

Misure di sicurezza Implementate nel software

Gestione credenziali di accesso

- User name: l'accesso al sistema avviene solamente attraverso l'identificazione univoca del soggetto che vi accede tramite username e password. 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: regole di complessità della password sono preimpostate nel sistema e sono configurabili in accordo con il titolare: si potranno scegliere diversi gradi di complessità da applicare a tutti gli utenti, sono configurabili anche i tempi di rinnovo delle password.
- Funzioni di blocco account a tempo oppure blocco account per superamento tentativi di login falliti sono preimpostate e configurabili in accordo con il Titolare.
- È possibile utilizzare anche una modalità two factor authentication tramite una ulteriore one time password inviata alla mail associata all'utenza.
- In alternativa alla gestione nativa delle credenziali sopra descritta, il sistema può essere configurato in modalità per cui la gestione delle credenziali e la loro validazione sono delegate ad un sistema terzo tramite SAML 2.0

Minimizzazione:

- Profili di autorizzazione: il Titolare può configurare l'accesso ai dati personali trattati nel sistema a seconda delle attività svolte dagli utenti, in alternativa la definizione dei profili viene implementata dal Responsabile su indicazioni del Titolare.

Identificazione di chi ha trattato i dati:

- Strumenti di log: sono presenti e attivi in maniera predefinita log che permettono di ricostruire le modifiche effettuate sulle utenze e sulla assegnazione dei profili alle utenze.
- Strumenti di log: vengono registrati gli eventi di login, logout e tentativi di login falliti, corredati dai dati di contesto disponibili (indirizzo IP di origine, browser utilizzato, etc).
- Strumenti di log: per le porzioni di dati personali anagrafici e organizzativi sono presenti log che permettono di risalire a chi e quando ha creato il record e chi e quando ha effettuato l'ultima modifica.
- Le utenze di servizio per personale che cura l'assistenza e l'esercizio del sistema sono nominali e seguono le stesse logiche di log accessi e profilazione validi per le altre utenze.

Tecniche di crittografia:

- Crittografia delle password: le password sono registrate in maniera crittografata, viene generato un hash con algoritmo SHA512 aggiungendo un "salt" di utente

- Crittografia della base dati: I dati a riposo e residenti in Database sono crittografati mediante gli strumenti standard messi a disposizione dal DBEngine, (TDE - Transparent Data Encryption).
- Dati in transito: i dati in transito sono crittografati utilizzando https/SSL.

Privacy by default

- Attivazione profilo utente: gli utenti sono attivati con uno o più dei profili autorizzativi definiti a cura del Titolare, autonomo nella scelta della profilazione utente idonea e nella attribuzione delle autorizzazioni in funzione dell'area omogenea di cui fa parte l'utente o del profilo di autorizzazione individuale. In alternativa, la profilazione degli utenti può essere svolata da consulenti applicativi su indicazioni del Titolare.
- Primo accesso: nei casi di gestione nativa delle credenziali, la password per il primo accesso viene generata in maniera casuale e recapitata esclusivamente al proprietario dell'utenza tramite email.

Diritti degli interessati:

- 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 sistema per cancellare l'anagrafica e i dati associati all'interno dell'applicativo.
- Per garantire il diritto dell'interessato ad avere informazione su quali dati tratta il Titolare e alla portabilità dei suoi dati, il Titolare può richiedere specifico supporto ai consulenti applicativi Bookmark.
- Il Cliente può anonimizzare i dati personali degli interessati tramite funzioni apposite o con il supporto di consulenti applicativi Bookmark. Queste operazioni riguardano le tabelle con esclusione dei campi discorsivi (note) e dei documenti (allegati) sui quali contenuti non è possibile attivare alcun controllo a livello di procedura.
- Eventuali altre richieste degli interessati possono essere espletate richiedendo specifico supporto ai consulenti applicativi Bookmark.

Salvo dove diversamente specificato, queste operazioni vengono eseguite dal Responsabile dietro indicazione da parte del Titolare

Misure di sicurezza per l'assistenza

Premessa

Autorizzazione tramite ticket

Gli addetti Bookmark possono effettuare attività di assistenza solo dietro richiesta del Titolare, che viene formalizzata attraverso l'apertura di un ticket sul sistema raggiungibile all'indirizzo https://support.bkm.it. L'apertura di un ticket vale anche come autorizzazione implicita:

- *per le operazioni di backup e trasferimento in locale dei dati il cui trattamento si rende necessario per le attività di assistenza.*
- *Per l'accesso ai dati del cliente, sotto qualunque siano strutturati (Server, Database, ecc.)*

Gli addetti che accedono ai dati sono nominati Amministratori di Sistema per gli ambiti specifici e necessari per lo svolgimento delle attività di assistenza.

Aree di assistenza

L'attività di assistenza può riguardare l'area applicativa, l'area dei Database e l'area infrastrutturale (server).

Utenze.

Affinché l'incaricato Bookmark possa effettuare tutte le attività necessarie sull'ambiente del Titolare, siano esse di start-up che di assistenza in esercizio, è necessario che venga appositamente creata un'utenza specifica e individuale all'interno del sistema.

Il prodotto viene installato da Bookmark con già presenti e preconfigurate le utenze personali per i vari addetti all'assistenza con diritti amministrativi.

La creazione di ulteriori utenze in ambito infrastrutturale (On Premise) deve essere richiesta al Titolare che, attraverso le sue utenze amministrative, potrà creare il nuovo utente.

Per la codifica delle utenze si consiglia di utilizzare l'indirizzo email dell'incaricato Bookmark, in modo che il Cliente potrà riconoscere la provenienza dell'utenza stessa.

Per la creazione di utenze applicative dovrà essere coinvolto il Titolare, il quale dovrà essere guidato all'accesso e alla creazione dell'utenza precisando e condividendo con lui, i diritti che verranno assegnati a quest'ultima.

Non devono mai essere configurate o utilizzate da parte dell'operatore utenze non personali o generiche, non riconducibili univocamente all'operatore stesso. È fatto divieto per gli operatori di accedere con credenziali afferenti ai colleghi.

Nel caso di assistenza applicativa l'addetto Bookmark può configurare l'accesso in maniera tale da assumere l'identità delle varie persone che possono essere coinvolte nel problema. In questo caso l'operazione di accesso ai dati viene registrata in capo all'utenza dell'addetto all'assistenza.

Chiusura del ticket

Al termine delle attività di assistenza (chiusura del ticket), il Titolare riceverà una email che comunicherà il termine delle stesse.

Assistenza on site

Gli addetti Bookmark accedono presso la struttura del Titolare per fare formazione od effettuare attività tecnica di manutenzione.

In questo caso gli addetti Bookmark lavorano come se facessero parte della struttura del Titolare ed adottano tutte le procedure di sicurezze implementate dallo stesso. I Titolari 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 Bookmark abbia la necessità di prelevare archivi o database di cui necessita per risolvere le problematiche evidenziate è necessario che informi il Titolari e registri tale attività sulla Nota di intervento:

Al termine dell'attività presso gli uffici Bookmark sarà informato il Titolare sulla soluzione adottata e sulla successiva cancellazione dell'archivio.

Qualora vi fosse la necessità di conservare gli archivi per il tempo necessario al collaudo della soluzione adottata, dovrà essere informato il Titolare sul tempo massimo di conservazione di tali archivi.

Assistenza telefonica

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

L'addetto Bookmark è comunque tenuto ad effettuare l'assistenza telefonica senza l'utilizzo di dispositivi di riproduzione audio in modalità vivavoce.

Assistenza tramite email / ticket web

L'addetto Bookmark non è autorizzato a farsi mandare le credenziali di accesso del Titolare via e-mail né tantomeno potrà salvarle sullo strumento di ticketing.

Qualora un Titolare invii le credenziali di accesso al suo ambiente senza richiesta del tecnico Bookmark è necessario che lo stesso risponda che non è autorizzato ad accedere ai sistemi con credenziali di altri utenti in quanto questa modalità viola il GDPR. Quindi il tecnico Bookmark dovrà richiedere credenziali individuali oppure collegamento da remoto tramite strumenti a ciò dedicati.

Nell'assistenza tramite e-mail i tecnici Bookmark inseriranno sempre nel testo del messaggio il disclaimer per rendere edotto il Titolare dell'informativa sintetica e dei recapiti a cui potrà rivolgersi per esercitare i suoi diritti o i diritti dei suoi interessati.

I tecnici Bookmark firmeranno ogni e-mail con nome e cognome e l'informazione sarà salvata nel ticketing.

Assistenza tramite ricezione di dati da clienti

Qualora per risolvere il problema segnalato dal Titolare fosse necessario avere una copia della base dati o di altri files o query contenenti dati personali è necessario procedere come segue:

- per i dati ospitati su strutture del Titolare, sarà possibile ricevere i files tramite Wetransfer o altri sistemi individuati dal Titolare o tramite Upload su area dedicata;
- Per i dati ospitati sui nostri sistemi Cloud SaaS, sarà possibile Ricevere i files tramite copia degli stessi.

Area Dedicata

L'area dedicata sarà impostata affinché il Titolare veda solo l'upload. Il download sarà visualizzato solo dal gruppo di assistenza a cui la richiesta di assistenza è stata effettuata.

Tre giorni dopo la data di pubblicazione una routine cancellerà i file caricati.

Scaricamento archivi tramite wetransfer o link di collegamento su ambienti del Titolare

In questo caso la gestione è in carico al Titolare che fornirà le credenziali per accedere all'ambiente dove risiedono gli archivi.

L'assistenza dovrà scaricarli in dischi locali, su una cartella non soggetta a backup e cancellarli al termine dell'attività come nelle altre ipotesi.

Autorizzazione di backup da parte dei nostri sistemisti

Nel caso di installazioni ospitate presso il nostro sistema Cloud Saas, l'addetto incaricato dell'assistenza chiederà ai tecnici di secondo livello di produrre una copia del database di produzione contenente i dati del Titolare, per potersi scaricare i dati in locale.

L'archivio ricevuto viene scaricato su una directory locale della postazione di lavoro dell'addetto Bookmark che si occupa dell'attività di assistenza. Tale cartella non è soggetta a backup. Gli archivi non possono essere salvati su dispositivi rimovibili.

L'operatore che ha in carico la gestione, terminata l'attività dovrà cancellare gli archivi ricevuti dal disco locale

Qualora vi fosse la necessità di mantenere gli archivi sarà mandata una e-mail al Titolare che ne darà l'autorizzazione.

Gli archivi dei Titolari non potranno mai essere trasmessi a gruppi di lavoro differenti rispetto a quelli finalizzati alla risoluzione del problema segnalato dal Titolare.

L'unica possibilità che i tecnici hanno per conservare gli archivi senza la prevista e preventiva autorizzazione del Titolare è l'anonimizzazione degli stessi.

Assistenza tramite collegamento remoto (software di condivisione desktop)

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 ci fa accedere ad un ambiente con profilo di autorizzazione da lui scelto per farci eseguire le attività di assistenza
- Il cliente può sconnetterci quando desidera.

Attraverso tali strumenti è possibile far accedere anche l'assistenza di secondo livello alla stessa sessione già aperta. In questo caso il cliente ne ha l'evidenza perché fornita dallo strumento e quindi accetta implicitamente tale modalità.

È obbligatorio utilizzare gli strumenti identificati da Bookmark in quanto licenziati e personalizzati 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 infrastrutture e dell'ufficio privacy è possibile utilizzare altri strumenti di connessione che si comportano in modo uguale.

Assistenza tramite collegamento remoto su IP Pubblici o VPN

Qualora l'attività di assistenza debba essere svolta su sistemi dei Titolari accessibili tramite connessione remota su rete pubblica (accesso via desktop remoto su IP pubblici oppure tramite VPN o accessi privati) è necessario che gli addetti Bookmark entrino nei sistemi dei Titolari:

- Previa autorizzazione del cliente;
- Previa ricezione delle credenziali individuali e le stesse siano state attivate per il tempo necessario all'esecuzione delle attività richieste;
- al termine dell'attività siano disattivate le credenziali da parte del Titolare.

L'accesso ai sistemi del Titolare avviene sempre a seguito dell'apertura di un ticket da parte dello stesso, che vale come autorizzazione implicita.

Attività di start-up progetti

Attività di start-up progetti con contratto

In questo caso le attività sono finalizzate ad adempiere all'obbligazione contrattuale e pertanto lecite (in questo caso non è prevista la creazione di un ticket da parte del cliente avente finalità autorizzative)

In questo caso è necessario redigere un documento di progetto in cui si convengono con il Titolare le modalità operative di esecuzione delle attività tra cui:

- Dati personali, archivi, base dati di cui necessita l'esecuzione delle attività;
- Dettaglio delle operazioni da eseguire sui dati;
- Identificazione del periodo entro cui sarà terminata tale attività;
- La previsione di un collaudo in cui il Titolare proverà la conversione.

I documenti che il Titolare ha sottoscritto per lo svolgimento di queste attività sono il contratto e la nomina a responsabile conferendo mandato a Bookmark di svolgere tutte le attività necessarie all'erogazione del servizio.

In questo caso non serve mandare al Titolare la lettera di incarico, in quanto la stessa viene fatta da Bookmark, in qualità di responsabile, agli addetti Bookmark.

Attività di start-up progetti senza contratto

In questo caso è necessario inviare al Titolare la nomina a responsabile al trattamento.

Nella nomina dovrà essere previsto un termine di svolgimento e portata a termine dell'attività. Bookmark provvederà ad incaricare gli addetti in qualità di responsabile.

Anche in questo caso è necessario prevedere una fase progettuale in cui condividere gli step sopra riportati.

Al termine sarà anche in questo caso essenziale prevedere il collaudo.

Con il documento di collaudo, che dovrà essere sottoscritto dal Titolare, lo stesso ci dichiarerà che le attività da noi effettuate sono corrette e quindi ci autorizzerà a cancellare i suoi archivi.

Nel documento di collaudo dovranno essere inserite le seguenti indicazioni:

- Il lavoro svolto è conforme rispetto all'ambito contrattuale convenuto;
- Il Titolare ha provato la conversione e dichiara che il prodotto funziona e tutte le funzioni sono state correttamente configurate e implementate;
- Che non ci sono errori nei dati convertiti e che quindi potrà utilizzare il prodotto per le finalità per cui lo ha acquistato.

Inoltre, il Titolare deve dichiarare che dalla data della firma del contratto non avrà nulla a pretendere rispetto all'attività di conversione svolta e prevista dal contratto e che autorizza Bookmark a cancellare ogni dato, archivio, data base che è servito per portare a termine la fase di ~~conversione~~ Avvio Progetto.

Solo qualora ci fosse la necessità di mantenere gli archivi del Titolare per finalità di cautela e verifica del lavoro da noi svolto, dobbiamo inviare una comunicazione con la quale il Titolare ci autorizza a conservare gli archivi per l'ulteriore periodo, terminato il quale gli archivi dovranno essere eliminati.

Tutto l'iter autorizzativo dovrà essere inserito nel post-vendita al fine di averne memoria.

Attività di assistenza in ambiente Cloud / SaaS

In questo caso le attività di assistenza si suddividono in attività di assistenza puntuale per la risoluzione di problemi e attività di natura sistemistica e infrastrutturale finalizzate alla manutenzione proattiva dell'ambiente di installazione.

Attività di assistenza per risoluzione problemi

Per le attività di assistenza finalizzate alla risoluzione di problemi valgono le considerazioni sopra esposte che qui si ricapitolano

Apertura del ticket

Gli addetti Bookmark possono effettuare attività di assistenza solo dietro richiesta del Titolare, che viene formalizzata attraverso l'apertura di un ticket sul sistema raggiungibile all'indirizzo https://support.bkm.it. L'apertura di un ticket vale anche come autorizzazione implicita:

- *per le operazioni di backup e trasferimento in locale dei dati il cui trattamento si rende necessario per le attività di assistenza.*
- *Per l'accesso ai dati del cliente, sotto qualunque siano strutturati (Server, Database, ecc.)*

Accesso individuale

Affinché l'incaricato Bookmark possa effettuare tutte le attività necessarie è necessario che venga appositamente creata un'utenza specifica e individuale all'interno del sistema a lui riconducibile ed è fatto divieto per gli operatori di accedere con credenziali afferenti ai colleghi.

Amministratore di Sistema

Gli addetti che accedono ai dati sono nominati Amministratori di Sistema per gli ambiti specifici e necessari per lo svolgimento delle attività di assistenza.

Attività di assistenza proattiva

Le attività di carattere proattiva sono finalizzate ad adempiere all'obbligazione contrattuale e pertanto lecite (in questo caso non è prevista la creazione di un ticket da parte del cliente avente finalità autorizzative).

I documenti che il Titolare ha sottoscritto per lo svolgimento di queste attività sono il contratto e la nomina a responsabile conferendo mandato a Bookmark di svolgere tutte le attività necessarie all'erogazione del servizio.

In questo caso non serve mandare al Titolare la lettera di incarico, in quanto la stessa viene fatta da Bookmark, in qualità di responsabile, agli addetti Bookmark.

In questo caso non serve la richiesta puntuale di autorizzazione al trattamento, implicitamente contenuta nella documentazione sopra identificata.

Documenti cartacei

Tutti i documenti contenenti dati dei Titolari stampati non possono essere riutilizzati come carta da riciclo e devono essere immediatamente distrutti.

Misure di Sicurezza per il Cloud

CODICE	CLASSE DELLA MISURA	LIVELLO DI APPLICAZIONE
M1	Sicurezza locali e apparati	I locali di BOOKMARK prevedono che l'accesso fisico ai locali sia consentito solo a personale autorizzato. Gli accessi vengono registrati.
M2	Autenticazione	I sistemi ed i servizi BOOKMARK sono accessibili solo attraverso il superamento di una procedura di autenticazione che prevede l'utilizzo di credenziali associate agli incaricati.
M3	Sistema di autorizzazione	L'accesso ai dati è controllato attraverso i profili di autorizzazione definiti a livello del sistema operativo della piattaforma che ospita l'applicazione e a livello applicativo.
M4	Controllo integrità dei dati	Sono attivi servizi di controllo per presenza di virus sia nei file systems locali dei singoli PC che nei file system condivisi, oltre che sui messaggi di posta elettronica.
M5	Backup e Ripristino dei dati	Sono in atto politiche di backup per i dati. Sono in atto attività indirizzate a ridurre il disservizio in caso di guasto (disasterrecovery)
M6	Gestione delle politiche di sicurezza	Sono predisposte delle Policy IT indirizzate alla sicurezza.
M7	Formazione degli incaricati	E' previsto un piano di formazione e di aggiornamento per gli incaricati di BOOKMARK e l'adozione di un regolamento per l'utilizzo dei sistemi informatici
M8	Supporti rimovibili	Sono disposte regole per la gestione (custodia, uso e riutilizzo) di supporti removibili in presenza di dati sensibili.
M10	Backup	Qualora sia applicata la crittografia sul db anche i backup sono crittografati;
M12	Data center	Le installazioni di BOOKMARK risiedono su Cloud Azure di Microsoft, nei datacenter West Europe (Amsterdam) e NORTH Europe (Dublin). Le misure di sicurezza fisiche sono consultabili al link https://learn.microsoft.com/it-it/azure/security/fundamentals/physical-security
M13	Comunicazione	Tutte le comunicazione da e verso l'esterno sono crittografate con protocolli HTTPS e/o IPSEC
M14	Amministratori di sistema	Bookmark ha adottato una politica operativa per gli Amministratori di Sistema
M16	VA	BOOKMARK ha adottato una politica per la conduzione di VA e PT

M17	Change management	BOOKMARK ha adottato una politica per la gestione dei cambiamenti sistemistici e per la gestione dei rilasci software
M20	Erogazione servizi Cloud	BOOKMARK ha adottato una Procedura per la gestione delle capacità
M24	Controllo prestazioni DC	BOOKMARK ha adottato una Procedura per gli indicatori
M25	Gestione incidenti	BOOKMARK ha adottato una procedura per la gestione degli Incident di Sicurezza informatica
M26	Disaster recovery	BOOKMARK ha adottato una Procedura Operativa per la gestione del Disaster Recovery
M28	Informazione operatori	BOOKMARK ha adottato un Regolamento per l'Utilizzo dei Sistemi Informatici
M31	Crittografia db	BOOKMARK ha adottato una Procedura per l'implementazione dei servizi di crittografia
M33	Diritti degli interessati	BOOKMARK ha adottato una procedura per l'esercizio dei diritti degli interessati
M35	By design	BOOKMARK ha adottato una Istruzione in tema di Privacy by Design
M36	Antivirus	BOOKMARK ha adottato una Procedura per il Malware
M37	Incarichi addetti	Gli accordi in essere con il personale prevedono una clausola di riservatezza
M38	Fornitori	BOOKMARK ha adottato una politica per la gestione dei fornitori
M40	Dispositivi rimovibili di memorizzazione e carta	Non vengono utilizzati in nessun caso per movimentazione di dati del Cliente; per Data Center possono essere utilizzati solo per attività legate all'installazione di patch/fix sui sistemi e per il backup delle password
M43	Modalità utilizzo strumentazione	BOOKMARK ha adottato un regolamento per l'utilizzo degli strumenti informatici
M46	VPN	Connessione tramite rete VPN Forticlient con connessione crittografata e protetta da credenziali di accesso
M54	SSO	I sistemi Cloud sono configurati con MFA – SSO tramite l'uso di Microsoft Authenticator
M55	Gestione credenziali di accesso	BOOKMARK ha adottato un sistema di procedure per la gestione delle credenziali di accesso sia per i propri collaboratori che per gli utenti delle applicazioni