2023

Disciplinare BYOD

BRING-YOUR-OWN-DEVICE

CORRETTO UTILIZZO DEI DISPOSITIVI DI PROPRIETÀ PERSONALE

CONSERVATORIO ROSSINI - PESARO

Sommario

Premessa 2
Art. 1. Oggetto e finalità del Regolamento 3
Art. 2. Principi generali 3
Art. 3. Condotta e utilizzo etico dei sistemi BYOD 4
Art. 4. BYOD (bring-your-own-device) 4
Art. 5. Navigazione Internet 5
Art. 6. Attuazione e controlli 5
Art. 7. Sanzioni 6
Art. 8. Decorrenza e pubblicità 6

Premessa

Le nuove modalità di lavoro in mobilità iniziate e, giocoforza implicitamente accettate nel periodo della pandemia, hanno di fatto svincolato l'utilizzo dei sistemi e dispositivi di proprietà personale, cosiddetti BYOD (*bring-your-own-device*), dagli impieghi tradizionali in ambito familiare a strumenti di lavoro dentro e fuori dell'organizzazione.

Mentre non sussistono problematiche di sorta nell'impiego dei dispositivi personali durante la normale prestazione lavorativa per finalità legate alle proprie mansioni come il controllo della posta elettronica, del sistema di gestione presenze o comunque di piattaforme legate alle attività svolte, sussistono invece problematiche non banali riguardanti la sicurezza del patrimonio informativo e, aspetto non secondario, le performance lavorative nel caso di utilizzi ludici e quindi indebiti come la navigazione Internet, la frequentazione dei social media, gli instant messaging (soprattutto nel caso dei gruppi di interesse), lo streaming audio o video.

Il confine non è facilmente individuabile poiché, vista la diffusione e la facilità di utilizzo, gli strumenti di messaggistica come WhatsApp sono da tempo utilizzati per le chat di ufficio, per lo scambio e la diffusione di informazioni di servizio o, addirittura, nell'ambito degli ordini di servizio.

Per quanto premesso, **è necessario regolamentare l'uso degli strumenti BYOD in modo da delineare gli impieghi in ambito lavorativo, evitando inutili sovraesposizioni in termini di condivisione di dati personali o utilizzi per finalità ludiche, non ammissibili durante il normale orario di servizio e incompatibili con il buon andamento dell'Amministrazione.**

Art. 1. Oggetto e finalità del Regolamento

1. Il presente Regolamento definisce il modello comportamentale considerato accettabile, per gli utilizzatori dei sistemi e dispositivi di proprietà personale, ovvero i cosiddetti BYOD (*bring-your-own-device*), impiegati dal personale dipendente in via esclusiva per tutte le attività, svolte on-line o in locale, legate all'espletamento delle proprie mansioni svolte presso il Conservatorio Rossini di Pesaro.
2. Al fine di preservare il patrimonio informativo dell'organizzazione, la continuità operativa dei servizi erogati e parallelamente ridurre i rischi di esposizione, sia dal punto di vista sanzionatorio che risarcitorio (tenuto conto delle normative nazionali ed europee vigenti, come il GDPR), **il Conservatorio Rossini di Pesaro richiede agli utilizzatori dei sistemi e dispositivi BYOD di conformarsi obbligatoriamente ai dettami del presente Regolamento.**

Art. 2. Principi generali

1. I principi ispiratori del presente regolamento sono i seguenti:
   a) Tutela dei diritti, delle libertà e della dignità delle persone;
   b) Garanzia della necessaria *continuità operativa* per l'erogazione del miglior servizio possibile unito al minor dispendio di energie (umane, tecnologiche, temporali ed economiche);
   c) Tutela del patrimonio informativo dell'organizzazione e riduzione dei rischi connessi al trattamento dei dati e quindi della probabilità di:
      i. Accessi illegittimi ai sistemi o agli applicativi;
      ii. Modifiche indesiderate alle informazioni;
      iii. Perdita della disponibilità dei dati;
   d) Conformità normativa e allineamento agli standard di mercato;
   e) *Security* e *privacy by design* ovvero considerare la sicurezza e la conformità alla protezione dati personali come parte integrante della progettazione complessiva del sistema;
   f) Approccio alla sicurezza di tipo multilivello (*Layered security*), adottando tecniche di segmentazione e segregazione quanto maggiormente possibile;
   g) Protezione del patrimonio informativo in ogni fase del trattamento e per tutto il ciclo di vita, ovvero quando i dati sono elaborati e comunicati ("*in transit*") o quando sono conservati ("*in storage*");
   h) Riduzione della superficie di esposizione rispetto alle vulnerabilità ovvero le debolezze sistemiche trasformabili in un evento indesiderato nel caso si attui una minaccia, partendo dal modello "tutto chiuso":
   i) Corretto bilanciamento tra usabilità e sicurezza, adottando contromisure basate sull'Analisi dei rischi;
   j) Adozione della Regola del minimo previlegio rispetto alla finalità (*separation of duties policy*), in ottica di stratificazione dei profili e degli accessi;
   k) Diritto alla disconnessione degli utilizzatori dai sistemi *mobile* al di fuori dell'orario di lavoro;
   l) Consapevolezza di tutti gli utilizzatori rispetto ai rischi e alle corrette modalità di utilizzo dei sistemi e dei servizi IT;
   m) Utilizzo dei BYOD da parte del personale dipendente, subordinato o parasubordinato ammesso per le sole attività legate alla prestazione lavorativa, incluse eventuali chat di gruppo nei sistemi di instant messaging per le sole comunicazioni di servizio; in ogni caso non sono ammessi utilizzi ludici, messaggistica continua con familiari, parenti o amici, navigazione Internet non connessa con l'attività lavorativa, ascolto e visione in streaming di audio o video.

Art. 3. Condotta e utilizzo etico dei sistemi BYOD

1. L'utilizzo dei sistemi e dispositivi BYOD in ambito lavorativo sono ammessi esclusivamente per condurre e supportare la missione dell'organizzazione, ovvero in tutte le attività legate agli ambiti tecnici e amministrativi.
2. Gli utenti sono responsabili dell'utilizzo dei sistemi e dispositivi BYOD in modo eticamente corretto, sicuro, legale e conforme al presente regolamento, tenendo nella massima considerazione i diritti, le libertà fondamentali, la sensibilità delle persone come anche gli obiettivi primari dell'organizzazione.
3. L'utilizzatore di sistemi e servizi IT è direttamente responsabile di tutte le attività effettuate con gli account dell'organizzazione assegnati, con particolare riguardo alle informazioni inviate o richieste, caricate o visualizzate nel proprio sistema e dispositivo BYOD.
4. In ambito lavorativo all'utilizzatore di sistemi e dispositivi BYOD sono tassativamente vietate le seguenti attività:
    a. La creazione o la trasmissione di qualsiasi materiale o documento, in qualsiasi formato, che possa essere ragionevolmente ritenuto offensivo, diffamatorio o osceno;
    b. La creazione o la trasmissione di materiale o documento in qualsiasi formato che possa ragionevolmente essere ritenuto suscettibile di molestare, intimidire, danneggiare o turbare qualcuno o qualcosa;
    c. La trasmissione non autorizzata di documenti etichettati come confidenziali su canali o sistemi non sicuri o non omologati dall'organizzazione;
    d. L'invio di dati di tipo sensibile su canali non sicuri come sistemi di instant messaging o file hosting;
    e. La creazione o la trasmissione di qualsiasi documento non riconducibile alle funzioni o ai compiti di competenza oppure estraneo alle attività dell'organizzazione;
    f. L'accesso non autorizzato ai sistemi o ai servizi IT;
    g. L'utilizzo per finalità personali dei sistemi o dispositivi BYOD durante il normale orario di servizio.

2) Gli utilizzatori di sistemi e servizi IT non sono autorizzati a rispondere a interviste telefoniche o sondaggi, compilare questionari on-line (anche quando sollecitati da importanti *brand*).
3) Gli strumenti *mobile* di tipo BYOD pongono il problema dell'equilibrio tra vita privata e vita professionale, data la progressiva trasformazione degli strumenti di comunicazione da asincroni a tempo reale. È riconosciuto all'utilizzatore il diritto alla disconnessione[1] dai dispositivi *mobile* al di fuori dell'orario di lavoro e dai turni di pronta disponibilità.
4) Anche nel caso dei sistemi di *instant messaging* (es. WhatsApp) vale il diritto alla disconnessione; è demandato alla sensibilità dei singoli il rispetto della distinzione tra tempistiche professionali e momenti da dedicare alla vita privata e familiare.

Art. 4. BYOD (bring-your-own-device)

1) I cosiddetti BYOD (*Bring Your Own Device*, letteralmente "porta il tuo dispositivo") possono essere utilizzati soltanto come sistemi isolati non collegati alla rete dell'organizzazione, a meno del Wi-Fi con accesso di tipo *guest* (ove presente). I sistemi di monitoraggio effettuano controlli automatici continui e segnalano al personale tecnico eventuali sistemi e dispositivi non catalogati e non autorizzati che abbiano effettuato un collegamento diretto alla rete locale dell'organizzazione (LAN). Eventuali sistemi o dispositivi non autorizzati collegati alla rete dell'organizzazione saranno bloccati e l'azione sarà considerata attacco al sistema informatico, segnalata alla Polizia Postale e delle

[1] Legge 6 maggio 2021, n. 61, di conversione del decreto-legge 13 marzo 2021, n. 30 riconosce esplicitamente al dipendente che lavora in modalità agile (o smart working) il diritto di disconnettersi dalle strumentazioni tecnologiche e dalle piattaforme informatiche utilizzate per svolgere la prestazione lavorativa.

Comunicazioni per la denuncia di reato di accesso abusivo a sistema informatico, ai sensi dell'Art. 615/ter del Codice penale.

2) È severamente vietato il collegamento alla rete dell'organizzazione di sistemi o dispositivi non distribuiti ufficialmente dai Sistemi Informativi. Il personale che effettuerà il collegamento diretto alla rete dell'organizzazione (sono escluse i Wi-Fi pubblici) sarà soggetto a sanzioni disciplinari. Saranno inoltre addebitati all'utilizzatore eventuali costi di ripristino o ulteriori danni che dovessero originarsi da un collegamento non autorizzato. Rientrano nei dispositivi del presente comma modem, router, switch, dispositivi wireless, Bluetooth o qualsiasi altro dispositivo che possa in qualche modo ampliare la superficie di esposizione e quindi i rischi connessi.
3) Il collegamento alla rete Wi-Fi pubblica dell'organizzazione (ove disponibile) dei dispositivi di proprietà personale come laptop, tablet o smartphone è possibile seguendo la specifica procedura di autorizzazione, registrazione e autenticazione. In tutti i casi è prevista la registrazione delle attività dell'utilizzatore e la navigazione Internet.
4) In conformità alla normativa vigente in tema di misure di protezione da adottare nelle attività di trattamento e considerata la non appartenenza di questa tipologia di dispositivi al perimetro di sicurezza dell'organizzazione, è vietato salvare dati personali raccolti durante le attività lavorative o comunque riferibili all'organizzazione sui BYOD, specialmente nel caso di dati di natura particolare.
5) Al fine di garantire un adeguato livello di sicurezza nell'utilizzo dei BYOD, anche per la sola consultazione delle piattaforme pubbliche (es. posta elettronica), comunque equiparabile a quello stabilito per l'organizzazione, è necessario che i tali dispositivi siano dotati almeno di antivirus con basi aggiornate, firewall locale attivo, aggiornamento del sistema operativo e dei componenti, assenza di software copiato o "*crackato*".
6) In nessun caso è possibile installare sui dispositivi BYOD software con licenza di proprietà dell'organizzazione.
7) Il trasporto al di fuori del perimetro dell'organizzazione di dispositivi di memorizzazione personali contenenti dati sensibili per l'organizzazione è vietato. Eventuali repliche o copie di sicurezza delle informazioni devono essere autorizzate e tracciate, secondo le procedure previste. La responsabilità in caso di perdita, smarrimento e involontaria diffusione dei dati contenuti nel dispositivo durante il trasporto al di fuori degli uffici, sarà attribuita all'utente titolare registrato.
8) Nell'ipotesi di smarrimento o furto di un dispositivo BYOD contenente dati personali riconducibili all'organizzazione titolare del trattamento dei dati, è obbligatorio comunicare l'accaduto al DPO/RPD per l'attivazione della procedura di *Data Breach.*

Art. 5. Navigazione Internet

1) Attraverso i dispositivi BYOD è tassativamente vietata la navigazione in siti Internet palesemente incompatibili con le finalità dell'organizzazione, che istighino a comportamenti illegali, che consentano o siano a rischio di diffusione di virus, cavalli di Troia o di altri programmi il cui obiettivo sia la distruzione, alterazione, sabotaggio, intercettazione, *hacking* o pirateria informatica a danno dei computer di altri utenti interni o esterni al perimetro dell'organizzazione.

Art. 6. Attuazione e controlli

1) I controlli di tipo indiretto, così come stabilito dalla disciplina sui controlli a distanza dei lavoratori[2], e i connessi trattamenti di dati personali lecitamente effettuabili dal datore di lavoro, sono comunque configurati in modo graduale, previo esperimento di misure comunque atte a garantire i

[2] Art. 4, l. 20.5.1970, n. 300 – Statuto dei lavoratori, incluse modifiche disposte dall'art. 23 del D.lgs. 151/2015

diritti degli interessati, escludendo attività idonee a realizzare controlli di tipo massivo, prolungato e indiscriminato dell'attività del dipendente stesso.

Art. 7. Sanzioni

1) Le operazioni effettuate in palese non conformità al presente Regolamento, esporranno alle sanzioni amministrative, civili e penali previste dalla normativa vigente.
2) Il mancato rispetto o la violazione di quanto previsto dal presente Regolamento, tenuto conto del principio di proporzionalità, è perseguibile con i seguenti provvedimenti:
    a. Comunicazione dell'illecito alla Direzione che provvederà all'applicazione di quanto previsto dal Codice Disciplinare
    b. Comunicazione alle Autorità competenti nel caso di evidenza di reati;
    c. Revoca o disabilitazione temporanea delle credenziali di autenticazione o di specifiche autorizzazioni.

Art. 8. Decorrenza e pubblicità

1. Il presente Regolamento entra in vigore a intervenuta esecutività della deliberazione di approvazione.
2. Il presente Regolamento è pubblicato sul sito web del Conservatorio Rossini di Pesaro.

Il Presidente
(Salvatore GIORDANO)
(Documento informatico firmato digitalmente ai sensi
del D.Lgs. 82/2005 s.m.i. e norme collegate,
il quale sostituisce il documento cartaceo e la firma autografa)