Kensington The Professionals' Choice™

Perché una politica sulla sicurezza fisica è parte integrante della **conformità al RGPD**

Limitazione di responsabilità: *Nessuna parte delle informazioni ivi riportate può essere interpretata come un consiglio legale. Le organizzazioni devono consultare un consulente legale per quanto riguarda la conformità al Regolamento generale sulla protezione dei dati o ad altre leggi o regolamenti applicabili.*

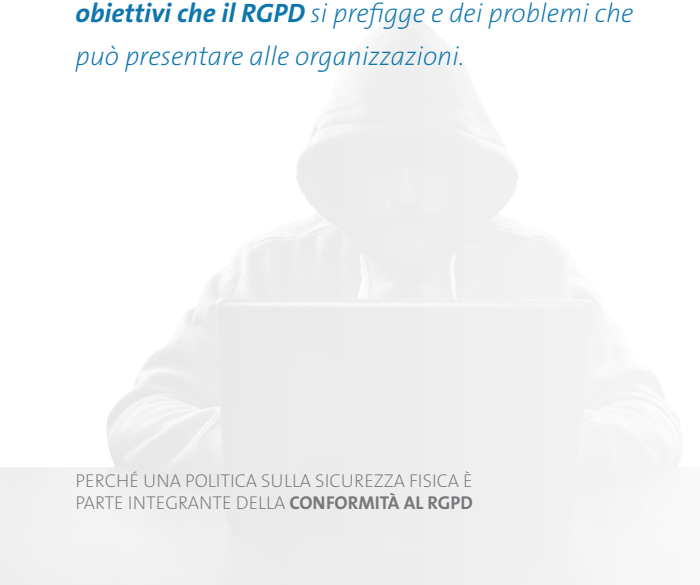
DATI protetti

Sommario

PERCHÉ UNA POLITICA SULLA SICUREZZA FISICA È PARTE INTEGRANTE DELLA **CONFORMITÀ AL RGPD**

Informazioni sul **presente documento**

*Questo libro bianco fornisce **una panoramica degli obiettivi che il RGPD** si prefigge e dei problemi che può presentare alle organizzazioni.*



PERCHÉ UNA POLITICA SULLA SICUREZZA FISICA È PARTE INTEGRANTE DELLA **CONFORMITÀ AL RGPD**

Lo scopo del presente documento è fornire un'introduzione al Regolamento generale sulla protezione dei dati (RGPD) dell'Unione Europea e alle modalità con cui influirà sulle diverse attività aziendali, in modo da poter delineare un quadro all'interno del quale sviluppare una politica sulla sicurezza dell'hardware per la propria attività in anticipo rispetto al regolamento, che entrerà in vigore a maggio del 2018.

Quindi, che cos'è il RGPD? Si tratta di un regolamento che richiede alle organizzazioni di adottare le buone pratiche in materia di protezione dei dati elettronici e cartacei e, in caso di violazione, di informare le persone interessate o potenzialmente interessate. La portata del RGPD si estende globalmente a tutte le organizzazioni che controllano o elaborano dati personali identificabili nell'UE, indipendentemente dall'area geografica di azione di tali organizzazioni. I requisiti del RGPD si applicano ai dati personali elettronici e cartacei e implicano che tutte le organizzazioni che trattano dati personali identificabili che hanno origine nell'UE debbano conformarsi ai requisiti del RGPD.

Proteggere i dati contro l'hacking e il malware è giustamente una priorità di molte organizzazioni, tuttavia molte di esse non riescono ad affrontare adeguatamente la questione della sicurezza fisica dell'hardware informatico. Più della metà non usa lucchetti fisici per l'apparecchiatura IT[1]. Tale situazione mette le organizzazioni a rischio di non conformità con il RGPD e le persone interessate a rischio di frodi e furti di identità. Tenendo presente questo aspetto, Kensington incoraggia le organizzazioni a riesaminare le proprie politiche e pratiche di sicurezza relative ai dati elettronici.

Una **panoramica**

Sebbene l'obiettivo principale del RGPD sia rafforzare i diritti della privacy online, la sicurezza fisica dell'hardware ricopre anch'essa un ruolo significativo.

Il RGPD si concentra sull'affrontare le sfide sempre più impegnative in materia di protezione dei dati e privacy, di esposizione a violazioni della sicurezza, hacking e altre forme di trattamento illecito dei dati.

*Questi punti **identificano le aree specifiche del RGPD** che rappresentano nuovi diritti o un rafforzamento dei diritti a favore delle persone fisiche.*

PERCHÉ UNA POLITICA SULLA SICUREZZA FISICA È PARTE INTEGRANTE DELLA **CONFORMITÀ AL RGPD**

1

Portabilità dei dati e "diritto all'oblio"

- Le persone fisiche adesso hanno il diritto di trasferire i propri dati personali da un'organizzazione all'altra.
- I dati personali devono essere forniti in un formato strutturato, leggibile da un computer.
- Una persona può richiedere la cancellazione o la rimozione dei propri dati personali.

2

Inventario

- Le autorità locali non devono essere più informate del fatto che vengono trattati i dati personali.
- Le organizzazioni devono, sotto la propria responsabilità, detenere una documentazione delle attività di elaborazione svolte.

3

Valutazione dell'impatto sulla protezione dei dati e sicurezza

- Le valutazioni dell'impatto sulla protezione dei dati consentono di identificare rischi elevati per la privacy delle persone.
- Le raccomandazioni e i requisiti relativi alla sicurezza dovrebbero basarsi su una valutazione del rischio.

4

Notifica di violazione dei dati

- Tutte le violazioni devono essere segnalate all'autorità di vigilanza.
- Anche le persone interessate dalla violazione devono essere informate.

5

Responsabilità e governance dei dati

- Le organizzazioni devono inoltre essere in grado di dimostrare la propria conformità al RGPD.

A chi si **applica?**

Qualsiasi organizzazione che detiene dati su cittadini dell'UE (indipendentemente dal fatto che la sede si trovi fuori dall'UE) è soggetta al RGPD; il regolamento si applica a tutti coloro che si occupano di tali informazioni.

PERCHÉ UNA POLITICA SULLA SICUREZZA FISICA È PARTE INTEGRANTE DELLA **CONFORMITÀ AL RGPD**

Il RGPD si applica alle organizzazioni, sia all'interno dell'UE che al di fuori dell'UE, che elaborano o controllano dati relativi a persone residenti nell'UE o cittadini dell'UE.

Il RGPD riguarda principalmente:

Titolari del trattamento dei dati: sono tenuti a indicare le modalità e le finalità per cui sono trattati i dati.

Responsabili del trattamento dei dati: persone che agiscono per conto del titolare del trattamento dei dati.

È responsabilità di queste due figure garantire che i loro clienti siano pienamente conformi a tutti gli aspetti del RGPD, al fine di evitare possibili sanzioni.

Una conformità efficace e dimostrabile al RGPD dovrebbe coinvolgere tutti i membri di un'organizzazione che si occupano di informazioni personali e sensibili. Ad esempio, quando un addetto alle vendite lavora in remoto, il suo computer portatile, che contiene informazioni sensibili sui clienti. dovrebbe essere dotato di misure di sicurezza fisica.

Un titolare o un responsabile del trattamento dei dati potrebbe avere bisogno di **nominare un Responsabile della protezione dei dati** e di tenere registri di tutte le attività di elaborazione che vengono eseguite per conto dei clienti.

Il RGPD riguarda i **dati personali** e i **dati personali sensibili** in formato elettronico e fisico

PERCHÉ UNA POLITICA SULLA SICUREZZA FISICA È PARTE INTEGRANTE DELLA **CONFORMITÀ AL RGPD**

Prima di redigere una politica di conformità aziendale, è importante considerare a quali tipi di dati si applica il RGPD.

I dati che rientrano nel campo di applicazione del RGPD includono tutte le informazioni su una persona identificabile e sono suddivisi in due categorie:

Informazioni personali, che includono dati come l'indirizzo e-mail o l'indirizzo fisico e tutte le informazioni che possono essere utilizzate come identificativo online, ad esempio l'indirizzo IP.

Informazioni personali sensibili, che includono informazioni più intime tra cui l'origine etnica, le opinioni politiche, la religione e la salute. In generale, le organizzazioni devono addurre motivi più convincenti per poter elaborare queste informazioni rispetto alle informazioni personali "normali".

Il RGPD riguarda le informazioni personali gestite dalle organizzazioni **in forma sia elettronica che fisica.**

Un quadro aziendale per la **conformità al RGPD**

Rivedendo gli aspetti relativi alle persone, ai processi e alle tecnologie, le organizzazioni potranno stabilire quadri chiari per una politica sulla sicurezza dei dati che contribuirà a garantire la conformità in tutte le aree del RGPD.

Al fine di conseguire la conformità al RGPD, le organizzazioni devono esaminare attentamente tre aree principali:

Persone: la titolarità e la responsabilità in capo al personale di tutti i dati da questi trattati all'interno dell'organizzazione sono fondamentali. L'organizzazione deve stabilire regole chiare per ciascun dipendente relativamente alla corretta gestione di tutti i dati elettronici detenuti all'interno dell'azienda. Queste norme applicano i requisiti del RGPD in merito al trattamento di tutti i dati. Ad esempio, è possibile introdurre regole chiare sull'utilizzo di dati sensibili archiviati sui computer portatili dei dipendenti e sul processo di cancellazione dei dati.

Processi: questo aspetto riguarda le procedure adottate all'interno dell'organizzazione, ad esempio come viene gestito l'utilizzo di dati, quali l'elaborazione e l'archiviazione dei dati relativi ai clienti. È fondamentale che le aziende rivedano tutti i loro processi attuali in materia di dati. Una volta individuate le lacune e le debolezze delle procedure attualmente in atto, l'organizzazione deve sviluppare un piano quadro volto a rafforzare o modificare questi aspetti, ove necessario, per assicurare la conformità al RGPD.

Tecnologia: le capacità e requisiti IT attuali dovrebbero essere anch'essi rivisti e adeguati di conseguenza entro maggio 2018. È compito di ogni organizzazione assicurarsi che tutti i sistemi esistenti che non supportano pienamente i regolamenti siano migliorati o sostituiti, per evitare di incorrere in sanzioni a seguito dell'entrata in vigore del RGPD.

Perché **la sicurezza fisica** è importante?

*Sebbene le minacce online e basate su software siano prioritarie per ogni organizzazione, sarebbe un errore ipotizzare che i **rischi relativi alla sicurezza fisica** siano scomparsi.*

PERCHÉ UNA POLITICA SULLA SICUREZZA FISICA È PARTE INTEGRANTE DELLA **CONFORMITÀ AL RGPD**

Dopo aver presentato i requisiti che il RGPD impone alle aziende, è opportuno affrontare la questione della sicurezza fisica dell'hardware all'interno delle organizzazioni e capire perché è una preoccupazione fondamentale per le imprese che si preparano a soddisfare i requisiti del RGPD.

Dopo le minacce online e la divulgazione involontaria dei dati, **dispositivi portatili** e **perdite fisiche** rappresentano le più grandi fonti di violazioni dei dati[2]:

Di media, ogni giorno, più di **5 milioni di dati vengono persi o rubati**[3] e più di **un terzo delle aziende non ha implementato una politica sulla sicurezza fisica** per proteggere computer portatili, dispositivi mobili e altri beni elettronici.[4]

Tenendo conto delle potenziali sanzioni delineate dal RGPD, di una forza lavoro sempre più mobile e della crescita delle postazioni di lavoro condivise, la sicurezza fisica dei computer portatili e dei dispositivi mobili è una precauzione razionale sia sul posto di lavoro che quando si è lontani da esso. Bloccare un dispositivo con un lucchetto è un modo rapido e semplice, nonché molto efficace, di prevenire eventuali furti.

Kensington offre una gamma completa di **soluzioni per la sicurezza** di una vasta gamma di computer portatili, inclusi i dispositivi senza slot di sicurezza. La gamma di valigie SecureTrek™ può essere fisicamente ancorata a qualsiasi oggetto fisso in ambienti quali aeroporti, hotel e fiere.

La sicurezza fisica resta responsabile **per molte comuni violazioni della sicurezza**

PERCHÉ UNA POLITICA SULLA SICUREZZA FISICA È PARTE INTEGRANTE DELLA **CONFORMITÀ AL RGPD**

Dei 697 incidenti correlati alla sicurezza dei dati registrati tra aprile e giugno del 2017 dall'autorità di vigilanza sulla protezione dei dati del Regno Unito, l'Information Commissioner's Office (ICO), il 6% è riconducibile al furto di un dispositivo non crittografato, mentre un ulteriore 3,5%[5] è costituito dai dati lasciati in un luogo non sicuro e dal furto dell'unica copia dei dati crittografati.

Nel **settore finanziario**, il 25% delle violazioni è dovuto a dispositivi smarriti o rubati che sono la causa più frequente della perdita di dati, essendo bersagli particolarmente allettanti a causa del volume dei dati sensibili archiviati e usati.[6]

Nel **settore sanitario**, il furto e la perdita fisica sono le cause principali degli incidenti correlati alla sicurezza e rappresentano il 32% degli oltre 100.000 incidenti rilevati in 82 paesi.[7]

Le capacità e requisiti IT attuali dovrebbero essere rivisti e adeguati di conseguenza entro maggio 2018. È compito di ogni organizzazione assicurarsi che tutti i sistemi esistenti che non supportano pienamente i regolamenti siano migliorati o sostituiti, per evitare di incorrere in sanzioni a seguito dell'entrata in vigore del RGPD.

La collaborazione degli utenti è critica per la conformità al RGPD

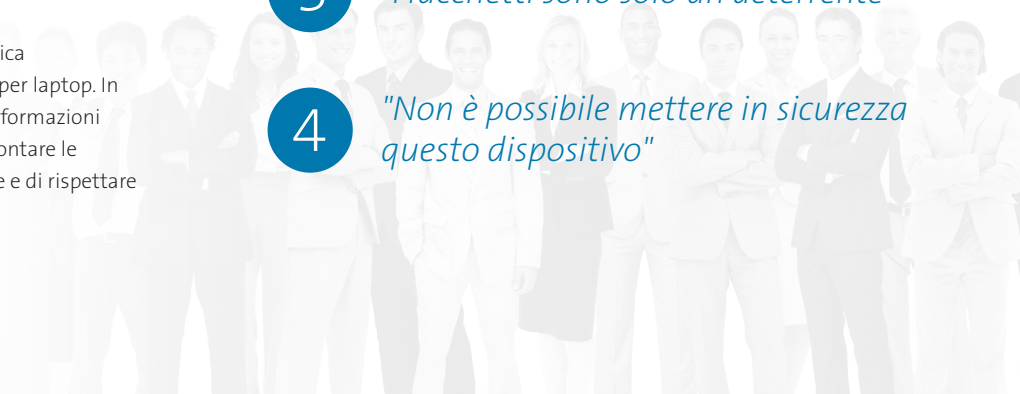
Se possiamo concludere che la sicurezza dei documenti cartacei rimane essenziale per la sicurezza delle informazioni, allora la domanda è: cosa possono fare le organizzazioni a questo riguardo?

Kensington è il leader mondiale nella sicurezza fisica dell'hardware IT, nonché l'inventore del lucchetto per laptop. In più di 35 anni Kensington ha acquisito preziose informazioni sulle esigenze, i desideri e le sfide che devono affrontare le organizzazioni che cercano di proteggere se stesse e di rispettare il RGPD.

PERCHÉ UNA POLITICA SULLA SICUREZZA FISICA È PARTE INTEGRANTE DELLA **CONFORMITÀ AL RGPD**

Tutte queste informazioni ci hanno portato a credere che vi siano quattro ostacoli e barriere principali per un'efficace sicurezza fisica all'interno delle organizzazioni:

1. *"Operiamo in un ambiente sicuro"*
2. *"Usiamo la crittografia e l'archiviazione su cloud"*
3. *"I lucchetti sono solo un deterrente"*
4. *"Non è possibile mettere in sicurezza questo dispositivo"*



Superare le barriere alla conformità al RGPD

PERCHÉ UNA POLITICA SULLA SICUREZZA FISICA È PARTE INTEGRANTE DELLA **CONFORMITÀ AL RGPD**

"Operiamo in un ambiente sicuro"

Telecamere a circuito chiuso, pass per i dipendenti e addetti alla sicurezza possono creare una sensazione di maggior sicurezza e un rischio percepito minore. Eppure il 58% dei computer portatili viene rubato negli uffici e l'85% dei responsabili IT sospetta furti interni.[8] I dati sono a rischio non appena il portatile viene rubato, soprattutto perché ne viene recuperato solo il 3%[9]. I lucchetti per computer portatili impediscono il furto opportunistico e consentono di risparmiare il tempo e i costi associati alla ricerca dell'autore del furto e alla sostituzione del computer portatile, per non parlare delle potenziali sanzioni ai sensi del RGPD.

"Usiamo la crittografia e l'archiviazione su cloud"

La crittografia non serve quando viene rubato un dispositivo che contiene dati di cui non è stato eseguito il backup. E anche se gli utenti non memorizzano i dati sui dischi rigidi, considerata la perdita di produttività di un dipendente che non ha più il proprio computer primario, vale la pena prendere misure adeguate di protezione. Basta fare una passeggiata nel luogo di lavoro per valutare con quale facilità un corriere, ad esempio, potrebbe rubare un dispositivo. Il 49% delle piccole e medie imprese impiega dai 2 a 4 giorni a sostituire un computer portatile smarrito o rubato.[8]

"I lucchetti sono solo un deterrente"

I lucchetti per computer portatili sono progettati principalmente per proteggere contro furti opportunistici. Ma sono anche molto efficaci per prevenire i furti in generale. In uno studio di IDC, il 52% dei responsabili IT che hanno subito furti di computer portatili ha affermato che i furti sarebbero stati evitati con un lucchetto.[8]

Superare le barriere alla conformità al RGPD

"Non è possibile mettere in sicurezza questo dispositivo"

Con il passaggio a modelli più sottili, i computer di oggi possono non incorporare il Kensington Security Slot™ standard di settore. Tuttavia, è errato pensare che tali dispositivi non possano essere fisicamente protetti. Anche i dispositivi senza uno slot di sicurezza possono essere bloccati con chiave per impedire furti opportunistici. Kensington offre una gamma completa di soluzioni per i più svariati dispositivi:

MicroSaver® 2.0 e ClickSafe® 2.0

Per i dispositivi che utilizzano il Kensington Security Slot™ standard, come il 90% dei dispositivi aziendali.

Kensington Security Slot™ su computer portatili e desktop

Il lucchetto MicroSaver® 2.0 si collega direttamente allo slot di sicurezza

Lucchetto ClickSafe® 2.0 collegato tramite ClickSafe Anchor

N17 per dispositivi Dell 2017

Per i dispositivi che utilizzano Wedge Security Slot, come i modelli Dell Latitude 2017 (e successivi) e altri dispositivi selezionati.

Wedge Security Slot

Computer portatile ancorato a un oggetto fisso

Lucchetto per laptop con chiave NanoSaver™

Per i dispositivi che utilizzano il Kensington Security Slot™ standard, come i dispositivi ultrasottili.

Kensington Nano Security Slot™

Lucchetti per laptop con chiave NanoSaver™

Soluzioni di sicurezza per Microsoft Surface™

Lucchetti specifici per dispositivi Surface™ Pro, Surface™ Book e Surface™ Studio.

Lucchetto con chiave per Surface™ Pro

Kit di sicurezza per Surface™ Studio

Staffa di sicurezza per Surface™ Book da 13,5”

Laptop Locking Station 2.0

Per i dispositivi senza slot di sicurezza, inclusi Surface™ Laptop e MacBook Pro®.

Laptop Locking Station con MacBook Pro®

Per trovare la soluzione di sicurezza ideale per ogni computer portatile o dispositivo è possibile visitare:
kensington.com/securityselector.com

6 punti chiave del RGPD da considerare

1. Valutare l'opportunità di nominare un Responsabile della protezione dei dati

Questa persona deve essere pienamente all'altezza delle responsabilità dell'organizzazione in materia di RGPD e avere una comprensione approfondita di quali informazioni, all'interno dell'organizzazione, sono "personali", dove sono archiviate, chi vi ha accesso, come individuare eventuali violazioni e a chi segnalare tali violazioni. **Il Responsabile della protezione dei dati non deve essere necessariamente un dipendente; questa funzione può essere è esternalizzata.**

2. Valutare il proprio sistema

Rivedere tutti i contratti, il supporto tecnico, le procedure e gli strumenti che riguardano l'elaborazione, il trattamento, l'archiviazione e la cancellazione dei dati per consentire di individuare eventuali debolezze o lacune che richiedono modifiche.

3. Sviluppare una strategia

Definire una nuova strategia che garantisca il pieno rispetto del RGPD. Questa può comprendere nuovi investimenti tecnologici, la revisione delle procedure del personale e della responsabilità dell'elaborazione dei dati nonché la creazione di nuovi ruoli all'interno dell'organizzazione.

PERCHÉ UNA POLITICA SULLA SICUREZZA FISICA È PARTE INTEGRANTE DELLA **CONFORMITÀ AL RGPD**

6 punti chiave del RGPD da considerare

4. Implementare una nuova politica aziendale

Il passo successivo per assicurare la conformità al RGPD è mettere in atto il piano a tutti i livelli dell'organizzazione. Investire nelle nuove tecnologie e nei sistemi richiesti sul posto di lavoro, presentarli al personale e pubblicare una guida informativa sulla gestione e il trattamento dei dati.

5. Coinvolgere i dipendenti

La nuova politica sulla conformità alle normative in materia di protezione dei dati deve essere presentata a tutto il personale, fornendo formazione, informazioni e supporto in modo che tutti i dipendenti siano istruiti e consapevoli dei cambiamenti che hanno luogo e della loro responsabilità nel garantire che l'azienda soddisfi i requisiti del RGPD.

6. Rivedere e migliorare

Una volta lanciato, il piano di conformità al RGPD deve essere riesaminato e migliorato prima che il regolamento entri in vigore. Riuscendo a individuare i miglioramenti necessari ben prima della data di entrata in vigore del RGPD, nel maggio del 2018, l'organizzazione si adatterà correttamente ed efficacemente ai cambiamenti e sarà completamente conforme.

Soluzioni

I lucchetti per computer portatili e dispositivi sono una risposta diretta alla necessità organizzativa di favorire la conformità dei dipendenti a una politica sulla sicurezza fisica dell'hardware e un modo per ridurre i rischi di potenziali violazioni della sicurezza. Soluzioni aggiuntive possono ulteriormente contribuire a ridurre questo rischio all'interno e all'esterno dell'ambiente di lavoro.

PERCHÉ UNA POLITICA SULLA SICUREZZA FISICA È PARTE INTEGRANTE DELLA **CONFORMITÀ AL RGPD**

Borsa SecureTrek™
La gamma SecureTrek™ di borse con ruote, valige e zaini consente di fissare questi prodotti in luoghi dove potrebbero verificarsi furti, ad esempio negli aeroporti, negli alberghi e nelle fiere.

Schermi per la privacy
L''hacking visivo' è facile, succede rapidamente e spesso non ce ne accorgiamo.[10] Uno schermo per la privacy, che restringe l'angolo di visualizzazione, contribuisce a ridurre tale rischio.

Lucchetti per porte USB
Gli amministratori di sistema possono impedire fisicamente agli utenti di collegare dispositivi USB ai computer, riducendo il rischio delle copie non autorizzate dei dati o di caricamento di malware nel sistema.

Armadietti
Un modo veloce e semplice per ricaricare, sincronizzazione e proteggere molti tablet e computer portatili ultra sottili.

VeriMark™ Fingerprint Key
Consente di accedere con i dati biometrici tramite Windows Hello™ in modo semplice, veloce e sicuro; funziona con servizi che richiedono l'autenticazione a due fattori, proteggendo dall'accesso non autorizzato e migliorando la sicurezza online.

Fonti

1. Sondaggio Kensington sul furto di computer portatili e sulla sicurezza IT, agosto 2016
2. Violazioni dei dati nel 2016 - Privacy Rights Clearinghouse
3. Indice del livello di violazioni, settembre 2017
4. Sondaggio Kensington sul furto di computer portatili e sulla sicurezza IT, agosto 2016
5. Information Commisioner's Office - https://ico.org.uk/action-weve-taken/data-security-incident-trends
6. Rapporto sulle violazioni nei servizi finanziari, Bitglass, 2016
7. Rapporto dell'indagine di Verizon sulla violazione dei dati del 2016
8. IDC Executive Brief 2010 - Laptop Theft: The Internal and External Threat
9. IDC White Paper 2007 - The Threat of Theft and Loss of Laptops for the SME
10. Esperimento di hacking visivo del Ponemon Institute, 2015

Kensington®

kensington.com

PER MAGGIORI INFORMAZIONI CONTATTARE:

Fulvio Luberto
ITA Sales Manager
fulvio.luberto@kensington.com
Mobile: +39 335 59 89 868

ACCO BRANDS

The Professionals' Choice™