GDPR INSIGHT

SERIES

SMART WORKING E TELELAVORO

ELEMENTI ESSENZIALI PER LA PIANIFICAZIONE DI SMART WORKING E TELELAVORO NEL RISPETTO DELLA NORMATIVA PRIVACY

NETPATROL

DATA PROTECTION & CYBER SECURITY

NET PATROL ITALIA

Siamo una società di consulenza specializzata in **privacy** e **cybersecurity**.

La nostra squadra è fatta da giuristi specializzati e professionisti della sicurezza delle informazioni, in grado di trattare in modo trasversale e organico le complesse tematiche che riguardano la protezione dei dati personali.

Il nostro **obiettivo** è dare alle aziende un interlocutore unico, capace di collaborare con il management per lo sviluppo e miglioramento di processi interni e sistemi di gestione finalizzati ad assicurare nel tempo la conformità alla normativa e un adeguato livello di sicurezza delle attività di trattamento.

- Privacy law
- Data Protection Officer
- Cybersecurity & Cyber law advisory

AFFILIAZIONI E CERTIFICAZIONI

INTRODUZIONE

Dal 25 maggio 2018 è applicabile nell'Unione Europea il Regolamento generale per la protezione dei dati personali (da ora in poi lo chiameremo **GDPR**).

L'adeguamento nazionale ha avuto completa attuazione con l'entrata in vigore del D.lgs. 101/2018, che ha modificato il Codice Privacy.

Il GDPR ha innovato tutta la gestione dei dati personali in Europa, dando il via ad un vero e proprio cambio di paradigma. Al suo centro, le persone e la responsabilizzazione delle aziende.

In questo episodio della serie **GDPR INSIGHT** approfondiremo gli elementi essenziali per pianificare al meglio modalità di lavoro da remoto, come smart working e telelavoro.

> Questo è un punto di partenza per coloro che vogliono individuare le aree chiave a cui è necessario prestare attenzione durante la pianificazione di modalità di lavoro da remoto.
>
> Ricorda però che il **GDPR** interessa un ambito molto più ampio rispetto ai temi qui affrontati.

Vorrei dare a dipendenti e collaboratori la possibilità di lavorare da remoto, cosa devo sapere?

Ci sono alcune questioni che è opportuno considerare prima di implementare modalità di lavoro da remoto:

- Qual è lo stato attuale dell'infrastruttura ICT aziendale?
- Qual è il livello di formazione attuale dei dipendenti in materia di privacy e sicurezza?
- Esistono già politiche interne che disciplinano l'uso delle risorse aziendali?
- Sarà necessario monitorare le attività dei dipendenti a distanza?
- Dovrò utilizzare soluzioni tecnologiche particolari e/o software as a service?

Notebook aziendale o personale?

Un parametro fondamentale quando si vuole dare la possibilità di lavorare da remoto, è decidere se i dipendenti lavoreranno con **strumenti aziendali** o **personali**.

Da un lato, consentire l'uso di strumenti personali può rendere l'esperienza di lavoro più proficua grazie alla familiarità con lo strumento, oltre a derivarne un risparmio economico per l'azienda.

D'altro canto, utilizzare strumenti personali potrebbe comportare dei rischi per la sicurezza dei dati.

Parola d'ordine: gestione del rischio

Lavorare da remoto è sempre più una necessità, e negli ultimi anni è diventato anche molto semplice.

Esistono soluzioni che in poco tempo e con poco sforzo permettono di impostare il lavoro da remoto.

La semplicità apparente però non deve ingannare. Il lavoro da remoto comporta diversi **rischi** sia per l'azienda che per i diritti dei dipendenti.

Pianificare il lavoro da remoto nel rispetto della **normativa privacy** (GDPR e Codice Privacy) può aiutare a mitigare molti di questi rischi.

GDPR E NORME RILEVANTI

PRENDIAMO CONFIDENZA CON LE BASI

LE REGOLE DEL GIOCO

Il GDPR trova applicazione ogni volta che sono raccolti e trattati dati personali. Per "dato personale" si intende **ogni informazione** riferibile a **persone identificate** o **identificabili**.

Per quanto riguarda gli argomenti qui trattati, il GDPR non è l'unica fonte da considerare:

- D.lgs. n. 196/2003, come modificato dal D.lgs. n. 101/2018 (Codice Privacy)
- L. 300/1970 (Statuto dei Lavoratori)
- Circolari INL (Ispettorato Nazionale Lavoro)
- Provvedimenti dell'Autorità Garante

Per ragioni di semplificazione, non scenderemo, di volta in volta, nel dettaglio delle fonti rilevanti.

Cosa c'entra il lavoro da remoto con il GDPR?

Il lavoro da remoto, a prescindere dalla tipologia (telelavoro, smart working…) pone diversi rischi per l'organizzazione che sceglie di implementarlo, sia dal punto di vista della **cybersicurezza**, che per quanto riguarda il rispetto della normativa **privacy**. Spesso nell'ambito del lavoro da remoto sono previste soluzioni tecnologiche che comportano il trattamento di dati personali dei dipendenti, che deve essere realizzato nel rispetto del GDPR.

Per sua natura il lavoro da remoto aumenta il rischio di **accesso non autorizzato** ai sistemi informativi aziendali e ai dati trattati. Oltre a questo, l'assenza del contesto aziendale potrebbe comportare un aumento degli errori umani, con rischio di **perdita** o **alterazione non autorizzata** di dati.

Il GDPR prescrive specifici obblighi sia per la sicurezza dei dati trattati dall'azienda (compresi anche quelli dei dipendenti), sia per quanto riguarda i principi applicabili ad ogni tipologia di trattamento.

Questo non significa che il lavoro da remoto sia da evitare, ma che è un'attività che va pianificata e gestita anche tenendo conto dei **requisiti privacy** e dei **rischi** per la sicurezza dei dati trattati dall'azienda.

Per **pianificare** correttamente un'iniziativa per il lavoro da remoto, fai attenzione ai seguenti punti:

	Gestisci adeguatamente i rischi, sia da un punto di vista organizzativo che tecnico
	Valuta la necessità e modalità di controllo a distanza dei dipendenti che lavorano da remoto
	Tratta i dati dei dipendenti in modo lecito, corretto e trasparente

PIANIFICAZIONE

MISURE ORGANIZZATIVE

LE PRINCIPALI MISURE ORGANIZZATIVE

Il lavoro da remoto richiede una pianificazione che tenga conto del contesto di partenza, degli obiettivi, delle risorse a disposizione e dei rischi. Vediamo quali sono le principali misure organizzative che possono essere adottate, nel rispetto del GDPR.

Prima di tutto: definizione degli obiettivi

Per lavorare da remoto non basta soltanto dare un pc portatile ai dipendenti. Prima ancora di partire, è necessario definire e adottare una politica interna che descriva nel modo più dettagliato possibile alcuni punti essenziali:

- ✓ **Condizioni d'uso** delle risorse aziendali accessibili da remoto
- ✓ **Modalità di collegamento** alle risorse aziendali
- ✓ **Limiti di utilizzo** degli strumenti di lavoro

E se i dipendenti useranno dispositivi personali per lavorare:

- ✓ Modalità di utilizzo dei **dispositivi personali** per fini lavorativi
- ✓ Sistemi operativi e software ammessi

Queste politiche interne, una volta definite e adottate, dovranno essere rese note ai dipendenti che lavoreranno da remoto.

Se possibile, prevedi un paio d'ore di formazione per assicurarti che tutti abbiano compresso le regole.

Definire queste regole minime aiuta a prevenire rischi per la sicurezza dei dati e agevola anche la tutela dei diritti dei dipendenti.

Un po' di formazione non guasta

Molte persone ancora non sono abituate a pensare al di fuori degli schemi lavorativi classici.

Per questo motivo potrebbero sottovalutare alcuni rischi derivanti dal lavoro in remoto.

Oltre alla definizione di politiche specifiche, sarebbe opportuno formare le persone in merito ai rischi, soprattutto se utilizzeranno dispositivi personali per fini lavorativi.

Tra i **rischi** più comuni quando si lavora in remoto:

- Furto o abuso delle credenziali di accesso ai sistemi informativi e servizi informatici aziendali
- Maggiore esposizione a virus e malware
- Maggiore esposizione a vulnerabilità software
- Maggiore tendenza a commettere errori, in assenza di confronto diretto con i colleghi

La sicurezza delle informazioni in un'azienda è fatta da persone che lavorano in modo **consapevole** e **competente**.

La consapevolezza è tanto più importante quando si lavora da remoto.

Non sottovalutare il cybercrime

L'industria del cybercrime è ormai una minaccia concreta e reale. Infezioni **malware** e tentativi di **phishing** sono all'ordine del giorno, e le difese software arrivano fino ad un certo punto.

Lavorare da remoto significa molto spesso accedere alle risorse aziendali attraverso **connessioni poco sicure**, che potrebbero essere sfruttate per ottenere accesso ai sistemi informativi aziendali.

È fondamentale che tutte le persone che lavorano da remoto siano consapevoli di questo, evitando di utilizzare **connessioni non sicure** come wi-fi pubblici o non protetti.

Se possibile, fornisci ai dipendenti che lavorano da remoto un **hotspot wi-fi** mobile configurato in modo sicuro, sulla base delle politiche aziendali.

Allo stesso modo, sarebbe preferibile evitare di lavorare in **luoghi pubblici**, dove malintenzionati possono acquisire informazioni semplicemente guardando il monitor della persona che sta lavorando.

Non dimenticare di aggiornare Registro e informative

Come visto, l'implementazione di smart working o telelavoro può comportare **nuove attività di trattamento**.

Le nuove attività di trattamento dovranno essere riportate nel **Registro** delle attività di trattamento, così come previsto dal GDPR.

Nel Registro dovranno essere indicate e descritte tutte le attività di trattamento, software utilizzati e se possibile le misure di sicurezza implementate.

Chiaramente, non dimenticare di aggiornare le **informative** per i soggetti interessati, avendo cura di indicare tutte le informazioni necessarie in relazione alle nuove attività di trattamento che svolgerai.

Data processing agreements e fornitori di servizi

Per agevolare il lavoro da remoto vengono spesso utilizzate soluzioni tecniche di tipo **software as a service**. I fornitori di queste soluzioni sono a tutti gli effetti **Responsabili del trattamento**, e questo comporta una serie di conseguenze giuridiche che richiedono attenzione:

	Scegli il fornitore sulla base delle garanzie offerte per il rispetto del GDPR. Il Titolare del trattamento ha l'onere di rivolgersi soltanto a fornitori in grado di dimostrare la conformità al GDPR. In mancanza, potresti essere responsabile in solido anche in caso di violazioni di legge commesse dal fornitore!
	Verifica l'ubicazione dei data center del fornitore. Se sono al di fuori dell'Unione Europea avrai bisogno di adottare alcune precauzioni contrattuali (o scegliere un altro fornitore)
	Verifica l'adeguatezza delle clausole contrattuali predisposte dal fornitore. Devono contenere tutte le disposizioni previste all'art. 28 del GDPR. In assenza, sarà necessario un contratto integrativo.

Alcune volte, la scelta di lavorare da remoto coinvolge anche soggetti diversi dai dipendenti, di cui bisogna tener conto.

Ad esempio, una scuola potrebbe decidere di svolgere **lezioni online**, con possibilità di registrazione delle stesse, chat di gruppo e autenticazione utenti.

In questo caso, i **dati personali** trattati non saranno soltanto quelli dei **docenti**, ma anche degli **studenti** che parteciperanno alle lezioni.

È possibile che gli studenti siano minorenni o comunque **soggetti vulnerabili**. Per questo, è estremamente importante scegliere un **fornitore affidabile**, che offra **adeguate garanzie** in merito al trattamento dei dati personali.

PIANIFICAZIONE

MISURE TECNICHE

LE PRINCIPALI MISURE TECNICHE

Nei fatti, il lavoro da remoto è fatto da strumenti e software che permettono al lavoratore di collegarsi alle risorse aziendali interne ovunque si trovi. Questa grande libertà comporta però anche dei rischi, che sono gestibili se vengono presi in considerazione durante la fase di pianificazione.

Dispositivi aziendali o personali?

I rischi sono diversi se per il lavoro da remoto si utilizzeranno dispositivi forniti direttamente dall'azienda o dispositivi personali.

La motivazione è semplice: i dispositivi personali sono molto eterogenei tra loro, e la loro configurazione è al di fuori del controllo dell'azienda.

Alcuni dipendenti potrebbero avere notebook con sistemi operativi non aggiornati, o peggio ancora fuori supporto. Altri potrebbero avere installato del software che per sua natura comporta dei rischi per la **cybersicurezza** aziendale.

Allo stesso modo, un dispositivo personale o una rete domestica potrebbero essere **compromessi** senza che la persona ne sia consapevole, rischiando così di compromettere tutta la rete aziendale.

Per questo motivo, per sviluppare un modello in grado di gestire minacce e rischi bisogna tenere in considerazione che tipo di dispositivi useranno le persone per lavorare da remoto.

Sistema operativo e antivirus

Prima di consentire l'uso di dispositivi personali per il lavoro da remoto, è fondamentale accertarsi che siano soddisfatti dei requisiti minimi di sicurezza, come:

- **Sistema operativo** recente e aggiornato con patch di sicurezza periodiche
- **Software antivirus** installato e periodicamente aggiornato

Se il dipendente non dispone di Sistema operativo adeguato o software antivirus aggiornato, potrebbe essere opportuno dotarlo di licenza per l'installazione del software, o di un pc aziendale configurato in modo sicuro.

Attenzione alle credenziali di autenticazione

Soprattutto quando si usa un pc personale per lavorare è fondamentale gestire le **credenziali di autenticazione** in modo adeguato.

Come detto, i dispositivi personali potrebbero essere compromessi all'insaputa di chi li utilizza, mettendo a rischio anche le credenziali di autenticazione usate per accedere ai sistemi informativi aziendali.

Come se non bastasse, è possibile che questi dispositivi vengano usati in ambito familiare, aumentando ancora di più i rischi di abuso delle credenziali di accesso.

Fortunatamente, mitigare questi rischi è semplice: basta dotare i dipendenti di **password manager**, software in grado di memorizzare in modo sicuro (eventualmente anche in Cloud) migliaia di credenziali di accesso.

Nel caso in cui i dipendenti debbano accedere a risorse particolarmente importanti per l'operatività o per la natura dei dati trattati, sarebbe opportuno implementare tecniche di **autenticazione multi-fattore**, così da mitigare rischi di abuso delle credenziali di autenticazione e accesso non autorizzato ai sistemi aziendali.

Come accedere alle risorse aziendali?

Se le risorse aziendali non sono in **Cloud**, per accedervi da remoto ci sono due soluzioni:

- Utilizzare una connessione **VPN**
- Installare un **software per il controllo remoto**

La VPN (Virtual Private Network) è una connessione privata con cui è possibile collegarsi direttamente alle risorse aziendali. Le connessioni tramite VPN sono cifrate ed ogni utente deve essere autenticato.

Una volta connessi con VPN, i dipendenti potranno **accedere direttamente** al server aziendale, e lavorare come se fossero alla loro scrivania.

L'alternativa è utilizzare software per il controllo remoto. Una volta installati su un computer, questi software permettono di **connettersi** e gestire questo computer tramite un altro computer, collegato al primo grazie all'accesso remoto (a distanza).

Questi software devono essere però scelti con cura e assicurare che possano fornire un **controllo centralizzato** degli accessi, onde evitare rischi di accesso non autorizzato ai sistemi aziendali.

La scelta e configurazione di software per l'accesso remoto non è sempre semplice e dipende anche dal contesto di applicazione.

Per questo motivo, la soluzione preferibile a lungo termine potrebbe comunque essere la VPN.

Approfittane per fare ordine!

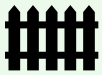
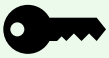
Potrebbe essere utile approfittare della pianificazione del lavoro da remoto per **censire** e **pre-autorizzare** tutti i **dispositivi** che si connetteranno alla rete aziendale o ai servizi informatici necessari per il lavoro.

Questa buona prassi, oltre che essere consigliabile in ogni caso, è particolarmente utile per tenere sotto **controllo** il perimetro aziendale, che nel caso di lavoro da remoto è inevitabilmente **distribuito** e geograficamente esteso.

Gestisci le identità digitali

Quando si lavora da remoto, l'unico modo che hai per evitare rischi di accesso non autorizzato alle risorse aziendali è assicurare una buona gestione delle **identità digitali**.

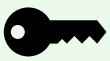
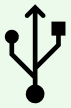
In particolar modo:

	Verifica periodicamente e amministra le identità digitali e credenziali di accesso dei dipendenti, **revocandole** quando necessario, ad esempio in caso di assenza prolungata.
	Verifica periodicamente i diritti di accesso e autorizzazioni secondo i principi di **minimo privilegio** e **separazione** delle funzioni. È molto frequente che in assenza di controlli gli utenti acquisiscano sempre più diritti di accesso nel corso del tempo (privilege creep).
	Accertati che le **utenze privilegiate** (es. amministratore di sistema) siano personali e custodite con cura. Queste utenze hanno le chiavi dell'azienda!

Le linee guida AgID per il lavoro da remoto nella Pubblica Amministrazione

L'Agenzia per l'Italia Digitale ha avuto modo di rilasciare alcune utili indicazioni per aiutare i dipendenti della Pubblica Amministrazione a svolgere attività di lavoro da remoto in sicurezza e nel rispetto della normativa vigente.

Vediamo insieme le 11 **raccomandazioni**:

	Segui prioritariamente le **policy** e le raccomandazioni dettate dalla tua Amministrazione
	Utilizza i **sistemi operativi** per i quali attualmente è garantito il supporto
	Effettua costantemente gli **aggiornamenti di sicurezza** del tuo sistema operativo
	Assicurati che i **software di protezione** del tuo sistema operativo (Firewall, Antivirus, ecc) siano abilitati e costantemente aggiornati
	Assicurati che gli **accessi al sistema operativo** siano protetti da una password sicura e comunque conforme alle password policy emanate dalla tua Amministrazione
	Non installare software proveniente da fonti/repository **non ufficiali**
	Blocca l'accesso al sistema e/o configura la modalità di **blocco automatico** quando ti allontani dalla postazione di lavoro
	Non cliccare su **link o allegati** contenuti in email sospette
	Utilizza l'accesso a **connessioni Wi-Fi** adeguatamente protette
	Collegati a **dispositivi mobili** (pen-drive, hdd-esterno, etc) di cui conosci la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione)
	Effettua sempre il **log-out** dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa

Per quanto di semplice applicazione, queste misure possono **aiutare** di molto a mitigare i più comuni rischi derivanti dal lavoro da remoto.

Seguirle costa poca fatica e i risultati sono assicurati.

CONTROLLO DEI DIPENDENTI

LICEITÀ, CORRETTEZZA E TRASPARENZA

DIRITTO DEL LAVORO E PRIVACY

Il controllo a distanza dei dipendenti è un campo di intersezione tra normativa sul lavoro e normativa privacy. Entrambe devono essere tenute in considerazione, ed entrambe prevedono alcune specifiche prescrizioni.

Posso controllare i dipendenti che lavorano da remoto?

Si può fare, ma ad alcune stringenti condizioni.

Per prima cosa, non dimenticare che controllare l'attività dei dipendenti significa **trattare dati personali**.

Ogni attività di controllo dovrà quindi rispettare la **normativa privacy** (GDPR e Codice Privacy per l'Italia).

Oltre alla normativa privacy bisogna tenere in considerazione lo **Statuto dei lavoratori**, che prevede espressamente alcune disposizioni proprio in merito all'attività di controllo del datore di lavoro.

Per quello che ci interessa, lo Statuto esprime tre concetti importanti:

	L'impiego di strumenti da cui deriva la possibilità di controllo a distanza dei lavoratori è possibile solo per esigenze **organizzative**, **produttive**, e di **sicurezza**. L'uso di questi strumenti deve essere approvato tramite **accordo sindacale** o **autorizzato da INL**.
	Questo non si applica però agli **strumenti di lavoro** e strumenti per la **registrazione delle presenze**, che potranno essere monitorati anche senza accordo sindacale o autorizzazione dell'INL.
Lo Statuto prevede infine che ogni attività di controllo debba rispettare la normativa privacy. In caso contrario, le informazioni raccolte saranno **inutilizzabili** e il datore potrebbe essere esposto alle sanzioni previste dal GDPR.	

Vediamo insieme quali sono le implicazioni pratiche del GDPR e dello Statuto dei lavoratori.

Quali sono gli strumenti di lavoro?

Gli strumenti di lavoro indicati dallo Statuto sono gli apparecchi, dispositivi, apparati e software che costituiscono un **mezzo indispensabile** al lavoratore **per eseguire** la **prestazione lavorativa**, e che per tale finalità sono messi a sua disposizione. Lo strumento, per rientrare nella nozione, deve essere utilizzato in via primaria ed essenziale per l'esecuzione dell'attività lavorativa.

Alcuni esempi:

	**Videosorveglianza**	Non può essere considerato uno strumento di lavoro, perché non è necessario e preordinato ad eseguire la prestazione lavorativa. Per installare un impianto di videosorveglianza servirà sempre accordo sindacale o autorizzazione INL.
	**GPS**	Dipende dal contesto! In alcuni casi il GPS può essere considerato uno strumento essenziale per l'esecuzione dell'attività lavorativa; in altri casi sarà invece implementato solo per motivi di sicurezza e tutela del patrimonio.
	**E-mail aziendale**	La posta elettronica aziendale messa a disposizione dal datore è sempre considerata uno strumento di lavoro e può essere controllata senza accordo sindacale o autorizzazione INL.

In alcuni casi capire se si è in presenza di uno **strumento di lavoro** non è semplice.

Deve essere considerato lo specifico contesto aziendale e gli specifici softwares utilizzati, che spesso sono delle vere e proprie soluzioni integrate che formano un sistema complesso e variegato.

Ad esempio, alcuni **CRM** utilizzati in ambito **call-center** sono costituiti anche da diverse funzionalità che esulano da quanto strettamente necessario ad eseguire la prestazione lavorativa e il cui unico scopo è valutare le **performance** dell'operatore. Per questo motivo non possono essere considerati meri strumenti di lavoro.

Sii trasparente e rispetta i diritti dei dipendenti

I dipendenti hanno il diritto di sapere se la loro attività lavorativa potrà essere monitorata a distanza, soprattutto nel caso di smart working, per il quale è prassi poter valutare il raggiungimento di certi obiettivi e le performance del lavoratore.

Informare i dipendenti non è soltanto una scelta di buon senso, ma una prescrizione normativa che deriva sia dal GDPR che dallo Statuto dei lavoratori.

In particolare, i dipendenti hanno il **diritto** di conoscere:

- ✓ L'elenco degli strumenti suscettibili di controllo a distanza
- ✓ La natura, estensione (anche temporale) e finalità del trattamento
- ✓ Le modalità con cui saranno trattati i loro dati personali, tempi di conservazione ed eventuali soggetti coinvolti nel trattamento

Il trattamento deve essere lecito e proporzionale

Monitorare l'attività dei dipendenti significa acquisire e trattare dati personali. Ogni attività di trattamento, di qualsiasi natura, deve fondarsi su una o più **condizioni di liceità**.

Il controllo a distanza, quando non strettamente necessario per eseguire la prestazione lavorativa, è tipicamente basato sul **legittimo interesse** del datore di lavoro, che può realizzare queste attività di trattamento senza il consenso del dipendente.

Il ricorso al legittimo interesse richiede però di effettuare un **giudizio di bilanciamento** tra gli interessi contrapposti di dipendenti e datore. Questo giudizio è una vera e propria analisi dei pro e contro delle soluzioni che si vorranno implementare, tenendo conto dei diritti dei dipendenti.

Ricorda che è comunque **vietato** il controllo indiscriminato, sistematico e su larga scala dell'attività dei dipendenti. Ogni attività deve avere una **finalità** determinata e lecita.

Valutazione dei rischi e DPIA

Prima di implementare soluzioni tecnologiche per il controllo a distanza dell'attività dei dipendenti è necessario realizzare una **valutazione d'impatto (DPIA)**.

La valutazione d'impatto è un processo con cui si esamina la **natura del trattamento** e si evidenziano i **rischi** per le persone, tenuto conto dei principi e prescrizioni del GDPR e della normativa nazionale. All'esito di queste valutazioni dovranno essere implementate **misure adeguate** a mitigare i rischi. Queste misure dovranno tener conto anche dei principi applicabili al trattamento, come i principi di minimizzazione e di limitazione della conservazione.

Ad esempio, nel caso di utilizzo di software per il **Mobile Device Management** (MDM) sarà necessario sottoporre il software e le relative attività di trattamento a valutazione d'impatto. Questi software possono infatti comportare un trattamento di dati personali molto invasivo, che deve tener conto dei diritti e libertà dei dipendenti. Tanto più se installati su **dispositivi ad uso promiscuo** (sia personale che lavorativo).

Net Patrol Italia

www.netpatrol.it - info@netpatrol.it - 02 87165913

Sede di Milano
Via Napo Torriani, 31 | 20124 Milano

Sede di Udine
Via Giovanni Paolo II, 3 | 33100 Udine

GDPR INSIGHT SERIES, N° 2

SMART WORKING E TELELAVORO

ELEMENTI ESSENZIALI PER LA PIANIFICAZIONE DI SMART WORKING E TELELAVORO NEL RISPETTO DELLA NORMATIVA PRIVACY

Marzo 2020

Disclaimer:

Questa pubblicazione non intende sostituire le fonti legali e riflette unicamente le opinioni degli autori.

Le azioni intraprese dalle organizzazioni non possono basarsi esclusivamente sulla lettura di questa pubblicazione.

In nessun modo la lettura di questa pubblicazione può sostituire il lavoro prestato da persone specializzate e competenti nella materia della protezione dei dati personali. Net Patrol Italia s.r.l. non può essere ritenuta responsabile per i danni o le violazioni del Regolamento UE 2016/679 realizzate dalle organizzazioni che fondino le proprie decisioni esclusivamente sulla base di questa pubblicazione.