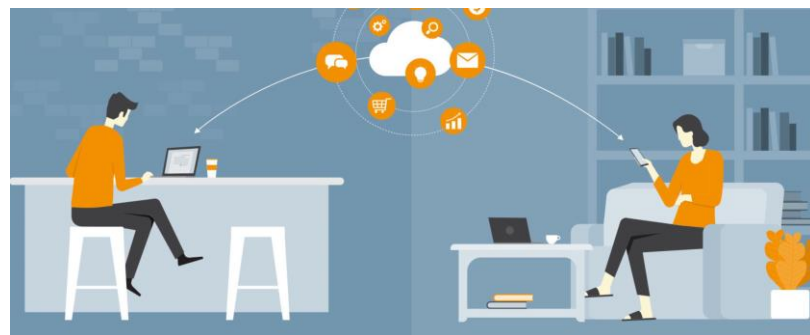


Privacy e sicurezza dei dati in modalità di lavoro smart working

Webinar per amministratori d'azienda ed emergenza Covid-19



Privacy, accountability e smart working nell'emergenza covid-19

A causa dell'emergenza sanitaria dovuta alla pandemia di coronavirus Covid-19, molte aziende hanno dovuto attivare modalità di lavoro agile utili a garantire la loro continuità operativa ...

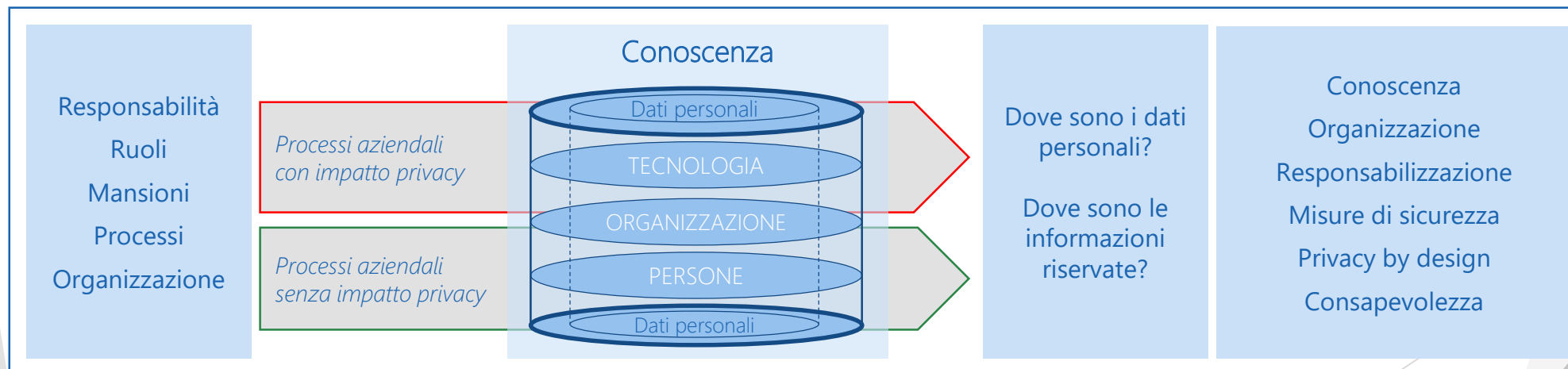
Smart Working come filosofia manageriale fondata **flessibilità** e **autonomia nella scelta degli spazi, degli orari e degli strumenti** da utilizzare a fronte di una maggiore **responsabilizzazione** sui risultati e sul lavoratore

Minor controllo sul lavoratore e sull'ambiente di lavoro del lavoratore -> **maggior rischio** per le informazioni

Scelta **organizzativa, tecnologica**, di **regole** condivise



Principio fondamentale del Regolamento Europeo 2016/679 – **General Data Protection Regulation** -
è la **responsabilizzazione del Titolare**: conoscere, organizzare e gestire i processi informativi dove sono presenti dati personali



Le misure di sicurezza organizzative e tecnologiche art. 32 GDPR

Le misure di sicurezza organizzative e tecnologiche adeguate che il Titolare deve definire ed applicare in base al proprio contesto, organizzazione, dimensione, rischio reale, dati personali trattati (*natura del dato*)

«Tenendo conto dello **stato dell'arte** e dei **costi** di attuazione, nonché della **natura**, dell'oggetto, del **contesto** e delle **finalità** del trattamento, come anche del **rischio** di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento mettono in atto **misure tecniche e organizzative adeguate** per garantire un livello di sicurezza adeguato al rischio»

Definire un insieme di regole e autorizzazioni al trattamento che tutta l'organizzazione deve seguire. Ad esempio:

- Policy password
- e-mail aziendale
- Internet
- Software aziendali
- Social media
- Elimina documenti
- Specifiche misure di sicurezza per dati più riservati

SICUREZZA FISICA

SICUREZZA INFORMATICA



Misure di sicurezza tecnico organizzative in modalità smart working

POSTAZIONE FISICA DI LAVORO, GESTIONE dei DOCUMENTI, VIDEO-CALL

- **Organizzazione:** postazione di lavoro dedicata
- **Riservatezza:** adeguata, evitare accessi non autorizzati, limitare interferenze, rumore, distrazioni, disturbi
- **Documenti cartacei:** non lasciare incustoditi, riposti in apposite teche / contenitori
- **Copie:** realizzare copie cartacee o digitali solo quando strettamente necessario
- **Eliminazione:** stracciare fisicamente il documento
- **Video-Call:** riservatezza e divieto di registrare o fare fotografie durante le videoconferenza se non con il consenso dei partecipanti

STRUMENTI INFORMATICI AZIENDALI

- **Utilizzo:** solo per lavoro
- **Sicurezza:** aggiornamenti richiesti dal sistema operativo
- **Antivirus:** utilizzare quello aziendale
- **Software:** non installare software non aziendali

STRUMENTI INFORMATICI PRIVATI

- **Sicurezza:** sistemi operativi per i quali è garantito il supporto
- **Antivirus:** installare un antivirus aggiornato

- **Wi-Fi:** adeguatamente protetto da password – evitare di utilizzare WI-FI pubbliche o libere
- **Accesso ai sistemi:** seguire le modalità definite dal Titolare (VPN; Cloud; Terminal Server; Remote Desktop,...)
- **Password:** policy password aziendale
- **Log-out:** in pausa, al termine della sessione di lavoro
- **Virus:** non cliccare su link o allegati contenuti in e-mail sospette (possibili cryptolocker, phishing, virus, frodi,...)
- **Chiavette USB:** collegare solo strumenti di cui si conosce la provenienza (nuovi, già utilizzati, forniti dal Titolare,...)
- **Salvataggio File:** son salvare in locale (desktop, disco locale, USB-drive, HD-esterno) in quanto manca back-up
- **Dubbi:** chiedere sempre al Titolare