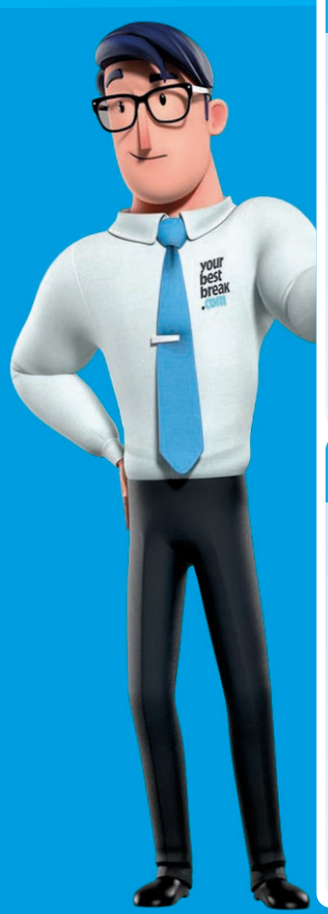
yourbestbreak.com

ISTRUZIONI PRIVACY

10 cose da ricordare per tutti



01 Hai letto e compreso le Istruzioni privacy?

Le istruzioni per il trattamento dei dati personali contengono disposizioni importanti che ogni autorizzato deve ben conoscere; le istruzioni, insieme alle istruzioni di lavoro, al Regolamento Aziendale Interno sull'uso delle postazioni di lavoro, sull'uso di Internet e della posta elettronica, sulla gestione degli incidenti di sicurezza e sulle violazioni dei dati (Data Breach) sono a disposizione nella rete **Intranet Aziendale.** Anche i modelli di Contratto, di Informativa ed i Termini di Servizio insieme a tutti gli altri documenti aggiornati sono disponibili nella **Intranet**. Se ci sono dubbi, domande o chiarimenti chiedere immediatamente a: **uffcioprivacy@ivsitalia.com**

02 Privacy "by design" significa ...

Considerare gli aspetti di Protezione dei Dati sin dalla progettazione di un processo o di un servizio è fondamentale per inserire le tutele per gli interessati direttamente nelle procedure e nella documentazione relative a quel particolare trattamento. Considera sempre gli **aspetti di sicurezza** quando stai pianificando un'attività, e se ritieni che ci possano essere delle criticità segnalalo ad un Responsabile! In particolare è necessario avvisare il dipartimento IT, i referenti della privacy per l'area o il DPO.

03 Proteggi le tue password ed ogni credenziale assegnata

Le **credenziali di accesso** a smartphone, tablet, pc, ed altri dispositivi aziendali oltre che ai sistemi di elaborazione non devono essere condivisi e devono prevedere opportuni livelli di complessità. Occorre utilizzare sistemi con autenticazione "forte" o a piu fattori, per le operazioni su dati particolari (sensibili e di profilazione). È buona abitudine usare password "forti" cioè composte da lettere (di cui almeno una maiuscola), numeri e caratteri speciali (!"£$%&/()=?). Qui [https://haveibeenpwned.com/Passwords] è possibile verificare se una password è sicura e se la propria email è presente nei data breach conosciuti.

04 Massima attenzione all'uso della posta elettronica!

La posta elettronica è un potenziale veicolo di intrusione da parte di malintenzionati che tentano di far arrivare virus o software malevoli (malware) quali ad esempio i **criptolocker o email di phishing** nelle quali chiedono informazioni sensibili o addirittura chiedono di fare delle attività mascherando il loro indirizzo email dietro a quello di un proprio superiore gerarchico o da parte di grandi aziende in genere banche, assicurazioni, società che forniscono servizi di telefonia e/o di pagamento In questi casi sospetti è obbligatorio porre grande attenzione per riconoscere se si tratta di situazione di pericolo reale ed allertare l'IT, o il proprio referente.

05 Rispetta il principio di pertinenza e necessità

La **minimizzazione** dei dati è uno dei cardini del GDPR. Limitare la tipologia e la quantità di dati trattati in rapporto alle finalità è un aspetto molto importante. Occorre quindi usare tecniche come la pseudonimizzazione e la crittografia quando si trattano Dati Particolari: a) sensibili (dati idonei a rivelare: origine razziale od etnica; orientamento religioso; orientamento sessuale; informazioni sullo stato di salute; adesione a partiti politici e/o a sindacati); b) di profilazione (derivati dalle nostre preferenze e abitudini di acquisto). Proteggi con una password i file word/excel o la cartella che li contiene. Se non sai come fare chiedi al dipartimento IT

06 Segnala ogni sospetta violazione di dati personali!

Se sospetti una **violazione di sicurezza** (iniziamo ad abituarci a chiamare gli attacchi ai dati ed alla business continuity aziendale: **Data Breach**) e se tale **Data Breach** comporta - accidentalmente o a seguito di illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali, segnalalo subito al tuo responsabile e/o all'ufficio Privacy ed IT di riferimento. Ricorda che ci sono SOLO 72 ORE per poter notificare il **Data Breach** al Garante e spesso è un OBBLIGO. Non sottovalutare mai situazioni sospette e non nascondere mai un avvenimento accidentale che possa generare un **Data Breach.**

07 Dubbi o segnalazioni? Contatta il DPO!

Il **DPO** (Data Protection Officer **dpo@dominio.ext**) anche detto Responsabile per la Protezione Dati e/o i vari Referenti Privacy che fanno parte dell'Organigramma Privacy sono a disposizione per ogni segnalazione relativa a sospetti Data Breach. Puoi confrontarti con il **DPO** per avere indicazioni sulle modalità per effettuare un trattamento conforme al **GDPR 2016/679**. È importante accrescere costantemente la cultura di protezione dei dati e del patrimonio di know-how aziendale, perciò non esitare a chiedere spiegazioni! Anche il **DPO** si aggiorna di continuo per migliorare le strategie e suggerire misure di sicurezza adeguate al rischio.

08 Informative e trasparenza: correttezza prima di tutto!

Le informazioni sul trattamento devono essere **chiare e comprensibili** per tutti. Ricordati sempre, sia da interessato che da persona autorizzata al trattamento (anche detto Soggetto Incaricato del Trattamento dei Dati da parte dell'Azienda, Titolare del Trattamento), che la trasparenza è fondamentale. L'informativa deve avere forma concisa, trasparente, facilmente comprensibile, con linguaggio chiaro e accessibile da tutti. È stato predisposto un modello di informativa per tutte le società del Gruppo che si può scaricare dal sito internet aziendale nella sezione Documentazione. Per qualsiasi chiarimento contatta il tuo **Referente Privacy**.

09 Conservazione dati: Per quanto tempo?

I dati vanno conservati in una forma che consenta **l'identificazione degli interessati** per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati: devi sempre considerare le policy aziendali per la conservazione dati. Se non sei sicuro, confrontati coi colleghi per conoscere le tempistiche specifiche. Questo è un tema complesso, introdotto dalle disposizioni del **GDPR 2016/679** in modo chiaro e l'applicazione pratica richiede un'analisi specifica effettuata per singola tipologia di trattamento, quindi prima di prendere decisioni in autonomia confrontati con il **DPO** o con il tuo Responsabile.

10 Evita di fare confusione e rispetta le regole!

Conoscere ed applicare i Principi della Protezione dei Dati è obbligatorio per ogni Organizzazione che deve dimostrare, con evidenze oggettive, che le misure poste in essere a tutela della sicurezza dei trattamenti sono adeguate ai rischi. Aver adottato idonee misure di sicurezza ai sensi dell'Art. 2050 del Codice Civile italiano, così come provare l'implementazione costante di misure fisiche, tecniche, logiche e procedurali adeguate al rischio, com'è detto nella formulazione dell'art. 32, equivale ad ottemperare al **principio di Accountability** che è la spina dorsale alla base del **Regolamento (UE) GDPR 2016/679.**