

## SIETE IN REGOLA CON LE MISURE MINIME DI SICUREZZA?

### CHECKLIST ADEMPIMENTI:

*I Titolari dei trattamenti di dati personali debbono adottare in ogni caso le seguenti misure minime di sicurezza, pena l'applicazione di sanzioni penali:*

<b>Trattamenti effettuati con PC, palmari, notebook ed altri strumenti elettronici</b>	<b>Si</b>	<b>No</b>
Autenticazione informatica degli accessi e adozione di procedure di gestione delle credenziali per l'accesso	<input type="checkbox"/>	<input type="checkbox"/>
1. Hai individuato e provveduto a nominare per iscritto gli incaricati, vale a dire le persone che operano il trattamento per tuo conto?	<input type="checkbox"/>	<input type="checkbox"/>
2. Hai fornito a ciascuno degli Incaricati un codice identificativo (user name) associato ad una parola chiave riservata (password), o una smart card o altro dispositivo o dato biometrico d'autenticazione, ad uso esclusivo del singolo Incaricato, per l'accesso ai dati da trattare?	<input type="checkbox"/>	<input type="checkbox"/>
3. Hai prescritto agli Incaricati di adottare le necessarie cautele per assicurare la segretezza della password e la diligente custodia dei dispositivi d'accesso ad uso esclusivo dell'incaricato?	<input type="checkbox"/>	<input type="checkbox"/>
4. Hai previsto che la password sia composta da almeno otto caratteri o altrimenti da un numero di caratteri pari al massimo consentito?	<input type="checkbox"/>	<input type="checkbox"/>
5. Hai verificato che la password non contenga riferimenti agevolmente riconducibili all'Incaricato?	<input type="checkbox"/>	<input type="checkbox"/>
6. Hai prescritto all'Incaricato di provvedere a modificare la password al primo utilizzo e, successivamente, almeno ogni tre mesi, se tratta dati personali sensibili, o almeno ogni sei mesi se tratta altri dati?	<input type="checkbox"/>	<input type="checkbox"/>
7. Hai verificato che il codice identificativo, ove utilizzato, non sia assegnato ad altri Incaricati, neppure in tempi diversi?	<input type="checkbox"/>	<input type="checkbox"/>

8. Hai verificato che codici, parole chiave e dispositivi d'autenticazione non utilizzati da almeno sei mesi debbano essere disattivati, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica?	<input type="checkbox"/>	<input type="checkbox"/>
9. Hai verificato che codici identificativi, password e dispositivi d'autenticazione per l'accesso ai dati siano disattivati nel caso in cui all'Incaricato non sia più consentito l'accesso ai dati personali?	<input type="checkbox"/>	<input type="checkbox"/>
10. Hai prescritto agli Incaricati di non lasciare incustodito e accessibile il PC, il notebook, il palmare o altra postazione elettronica durante una sessione di lavoro?	<input type="checkbox"/>	<input type="checkbox"/>
11. Hai impartito disposizioni scritte sulle modalità d'accesso alla postazione di lavoro e a dati in caso di prolungata assenza o impedimento dell'Incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità d'operatività e di sicurezza del sistema?	<input type="checkbox"/>	<input type="checkbox"/>
12. Hai organizzato la custodia delle copie delle credenziali in modo da garantire la relativa segretezza ed individuato preventivamente per iscritto i soggetti incaricati della loro custodia?	<input type="checkbox"/>	<input type="checkbox"/>
13. Hai prescritto loro di informare tempestivamente l'incaricato dell'intervento effettuato?	<input type="checkbox"/>	<input type="checkbox"/>

Ricorda che:

- Le parole chiave possono riferirsi a uno specifico trattamento o a un insieme di trattamenti.
- Le credenziali d'autenticazione consistono in un codice per l'identificazione dell'incaricato associato ad una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo d'autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato ad un codice identificativo o ad una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata ad un codice identificativo o ad una parola chiave.
- In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi, anziché ogni sei mesi.
- I dati sensibili sono dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o d'altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

<b>Adozione di sistemi d'autorizzazione all'accesso</b>	<b>Si</b>	<b>No</b>
1. Hai previsto un sistema di autorizzazione per disciplinare diversi ambiti e modalità di accesso degli Incaricati?	<input type="checkbox"/>	<input type="checkbox"/>
2. Hai individuato preventivamente i profili d'autorizzazione in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento?	<input type="checkbox"/>	<input type="checkbox"/>
3. Hai programmato di verificare periodicamente, e comunque almeno una volta l'anno, che persistano i presupposti per il profilo d'autorizzazione di ciascun Incaricato?	<input type="checkbox"/>	<input type="checkbox"/>

Ricorda che:

- Quando intendi distinguere i profili di autorizzazione all'accesso secondo gli Incaricati devi dotarti di un sistema d'autorizzazione
- Puoi individuare i profili di autorizzazione per classi omogenee di Incaricati, anziché con riferimento al singolo Incaricato

<b>Aggiornamento periodico dell'individuazione dell'ambito del trattamento</b>	<b>Si</b>	<b>No</b>
1. Hai programmato di verificare periodicamente, e comunque almeno una volta l'anno, l'ambito di trattamento di dati personali consentito a ciascun Incaricato?	<input type="checkbox"/>	<input type="checkbox"/>
2. Hai programmato di verificare periodicamente, e comunque almeno una volta l'anno, la lista degli Incaricati?	<input type="checkbox"/>	<input type="checkbox"/>
3. Hai programmato di verificare periodicamente, e comunque almeno una volta l'anno, l'ambito di trattamento di dati personali consentito agli addetti alla gestione e/o alla manutenzione dei sistemi informativi, hardware, software e database?	<input type="checkbox"/>	<input type="checkbox"/>
4. Hai impartito istruzioni organizzative e tecniche per la custodia e l'uso di floppy disk, cd-rom o altri supporti rimovibili sui quali hai memorizzato dati sensibili o giudiziari al fine di evitare accessi non autorizzati o trattamenti non consentiti?	<input type="checkbox"/>	<input type="checkbox"/>
5. Hai impartito istruzioni per distruggere o rendere inutilizzabili i floppy disk, cd-rom o altri supporti rimovibili sui quali hai memorizzato dati sensibili o giudiziari al fine di evitare accessi non autorizzati o trattamenti non consentiti?	<input type="checkbox"/>	<input type="checkbox"/>
6. Hai disposto che floppy disk- cd-rom ed altri supporti rimovibili contenenti dati sensibili o giudiziari e non utilizzati siano distrutti o resi inutilizzabili?	<input type="checkbox"/>	<input type="checkbox"/>
7. Hai adottato idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni?	<input type="checkbox"/>	<input type="checkbox"/>

Ricorda che:

- La nomina degli Incaricati va effettuata per iscritto
- La nomina deve individuare puntualmente l'ambito di trattamento consentito.
- La nomina può avvenire anche mediante documentata assegnazione della persona fisica ad un'unità operativa per la quale sia stato individuato per iscritto l'ambito di trattamento consentito ai relativi addetti.
- Puoi redigere la lista degli Incaricati anche secondo classi omogenee di incarico e dei relativi profili di autorizzazione
- Dati giudiziari si considerano tutte quelle informazioni, quali gli estratti del casellario giudiziale, il certificato dei carichi pendenti, le informazioni di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o le informazioni da cui si desume la qualità di imputato o di indagato dell'interessato.
- Floppy disk, cd.Rom e altri supporti contenenti dati sensibili o giudiziari possono essere riutilizzati da altri Incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono comprensibili e tecnicamente non ricostruibili in alcun modo.

<b><i>Protezione degli strumenti elettronici e dei dati</i></b>	<b><i>Si</i></b>	<b><i>No</i></b>
1. Hai predisposto idonei dispositivi e programmi elettronici per la protezione dei dati dal rischio di intrusione e dell'azione di software volti a danneggiare e/o interrompere il funzionamento dei sistemi informatici?	<input type="checkbox"/>	<input type="checkbox"/>
2. Hai prescritto l'aggiornamento dei dispositivi anti intrusione e antivirus almeno ogni sei mesi?	<input type="checkbox"/>	<input type="checkbox"/>
3. Hai previsto idonei strumenti di protezione dei dati sensibili e giudiziari contro l'accesso abusivo?	<input type="checkbox"/>	<input type="checkbox"/>
4. Hai programmato almeno ogni sei mesi, se tratti dati sensibili o giudiziari, o altrimenti almeno ogni anno, l'aggiornamento periodico dei software per prevenire la vulnerabilità dei tuoi sistemi informativi e correggerne i difetti?	<input type="checkbox"/>	<input type="checkbox"/>
5. Hai impartito istruzioni organizzative e tecniche per il salvataggio dei dati con frequenza almeno settimanale?	<input type="checkbox"/>	<input type="checkbox"/>

<b>Documento Programmatico sulla sicurezza dei dati sensibili e giudiziari</b>	<b>Si</b>	<b>No</b>
1. Hai scadenzato al 31 marzo di ogni anno il termine per l'aggiornamento del Documento Programmatico sulla sicurezza dei sensibili o giudiziari?	<input type="checkbox"/>	<input type="checkbox"/>
2. Hai predisposto l'elenco dei trattamenti di dati personali?	<input type="checkbox"/>	<input type="checkbox"/>
3. Hai provveduto alla distribuzione dei compiti e delle responsabilità nell'ambito delle strutture della tua azienda preposte al trattamento dei dati personali?	<input type="checkbox"/>	<input type="checkbox"/>
4. Hai disposto l'analisi dei rischi che incombono sui dati?	<input type="checkbox"/>	<input type="checkbox"/>
5. Hai individuato le misure da adottare per garantire l'integrità e la disponibilità dei dati?	<input type="checkbox"/>	<input type="checkbox"/>
6. Hai individuato le misure da adottare per la protezione delle aree e dei locali rilevanti ai fini della custodia e dell'accessibilità ai dati?	<input type="checkbox"/>	<input type="checkbox"/>
7. Hai predisposto criteri, procedure e modalità di disaster recovery per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento?	<input type="checkbox"/>	<input type="checkbox"/>
8. Hai previsto interventi formativi degli Incaricati del trattamento, per renderli edotti: a) dei rischi che incombono sui dati b) delle misure disponibili per prevenire eventi dannosi c) dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività d) delle responsabilità che ne derivano e) e delle modalità per aggiornarsi sulle misure minime adottate dal titolare?	<input type="checkbox"/>	<input type="checkbox"/>
9. Hai programmato la formazione di ciascun Incaricato al momento dell'ingresso in servizio in azienda?	<input type="checkbox"/>	<input type="checkbox"/>
10. Hai programmato la formazione di ciascun Incaricato in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento di dati personali?	<input type="checkbox"/>	<input type="checkbox"/>
11. Hai individuato i criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della tua struttura?	<input type="checkbox"/>	<input type="checkbox"/>
12. Hai acquisito dai soggetti esterni ai quali ti sei rivolto per l'adozione delle misure minime di sicurezza dei dati personali la descrizione scritta dell'intervento effettuato e l'attestazione della sua conformità alle disposizioni del Disciplinare Tecnico previsto dal Codice sulla privacy?	<input type="checkbox"/>	<input type="checkbox"/>
13. Hai programmato di riferire nella relazione accompagnatoria del bilancio di esercizio della tua società l'avvenuta redazione del Documento Programmatico sulla sicurezza?	<input type="checkbox"/>	<input type="checkbox"/>

<b>Trattamenti senza l'ausilio di strumenti elettronici</b>	<b>Si</b>	<b>No</b>
1. Hai impartito istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali?	<input type="checkbox"/>	<input type="checkbox"/>
2. Hai previsto l'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli Incaricati?	<input type="checkbox"/>	<input type="checkbox"/>
3. Hai disposto che atti e documenti contenenti dati personali sensibili o giudiziari siano controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione e siano restituiti al termine delle operazioni affidate?	<input type="checkbox"/>	<input type="checkbox"/>
4. Hai disposto che l'accesso agli archivi contenenti dati sensibili o giudiziari sia controllato?	<input type="checkbox"/>	<input type="checkbox"/>
5. Hai previsto che le persone ammesse, a qualunque titolo, dopo l'orario di chiusura degli archivi contenenti dati sensibili o giudiziari siano identificate e registrate?	<input type="checkbox"/>	<input type="checkbox"/>
6. Se gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, hai disposto che le persone che vi accedono siano preventivamente autorizzate?	<input type="checkbox"/>	<input type="checkbox"/>

Ricorda che:

- La lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Attenzione!

I Titolari del trattamento non possono limitarsi ad adottare le misure minime individuate dalla legge e volte ad assicurare un livello minimo di protezione dei dati personali, ma debbono adottare caso per caso tutte le misure idonee ad assicurare la sicurezza dei dati trattati e ad evitare la perdita e/o la sottrazione dei dati ovvero accessi non autorizzati, rimanendo altrimenti responsabili in sede civile.