

I SOGGETTI OBBLIGATI AGLI ADEMPIMENTI PRIVACY

Mod.	OBBLIGHI	TITOLARI SOGGETTI ALL'ADEMPIMENTO
1/2	Lettera informativa per i clienti e fornitori	Obbligatoria per tutti per rapporti instauratasi prima del 7 dicembre 2011. Non sussiste l'obbligo di farsi restituire il documento firmato per accettazione <u>a meno che</u> il titolare non tratti direttamente i dati sensibili dei propri clienti. Dal 7 dicembre 2011 è obbligatoria solo per persone fisiche (sono escluse società e ditte individuali).
3	Lettera informativa (comprensiva di consenso al trattamento dei dati) per i dipendenti	Solo per i Titolari che hanno almeno un dipendente regolarmente assunto.
4	Lettera di nomina a incaricato del trattamento	Tutti, ad eccezione delle attività gestite da un'unica persona.
5	Lettera di nomina a responsabile interno del trattamento: Nessuno. La nomina a responsabile è sempre facoltativa. Se ne consiglia l'adozione per realtà con oltre 15 dipendenti. Se il responsabile non è nominato è da intendersi come responsabile il titolare del trattamento .	La nomina scritta a responsabile è sempre facoltativa. Se ne consiglia l'adozione per realtà con almeno 15 dipendenti.
6	Lettera di nomina a responsabile esterno del trattamento	La nomina a responsabile è sempre facoltativa. Se ne sconsiglia sempre l'uso, tranne alcuni casi particolari.
7	Lettera di richiesta di consenso al trattamento per i Clienti	Solo per attività che comportano il trattamento di dati sensibili e/o giudiziari, es: studi medici o dentistici, agenzie di assicurazione, avvocati, commercialisti, ecc...
	Misure Minime per strumenti cartacei (cassetti e armadi chiusi a chiave)	Tutti
8	Lettera di garanzia per fornitori che trattano dati per conto del Titolare	Solo per coloro che affidano a dei fornitori esterni il trattamento di dati personali di cui sono in possesso (es: servizio paghe e contributi, medico aziendale, manutentore sistemi informativi, imprese di pulizie ecc...).
9	Nomina incaricato custode password	Modulo da allegare al modulo 4

10	Informativa Sito	Tutte le aziende che hanno un sito internet, la lettera va pubblicata sul sito.
11	Notificazione al Garante	<p>Solo chi effettua uno o più di questi trattamenti:</p> <p>a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;</p> <p>b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffuse, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;</p> <p>c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;</p> <p>d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;</p> <p>e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;</p> <p>f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.</p>

12

Misure Minime per strumenti elettronici (password, antivirus, firewall, sistemi di back-up, sistemi di autorizzazione).

Password : la password deve essere composta da almeno otto caratteri, non deve contenere nomi comuni, nomi di persone o riferimenti agevolmente riconducibili all'incaricato. Deve essere modificata dall'incaricato al primo utilizzo; successivamente deve essere modificata con cadenza semestrale, nel caso di trattamento dati sensibili la password deve essere modificata con cadenza almeno trimestrale.

Antivirus : deve essere installato, attivo e aggiornato.

Firewall : Apparato di rete hardware o software che filtra tutti i dati entranti ed uscenti, da e verso una rete o un computer, applicando regole che contribuiscono alla sicurezza della stessa.

Sistemi backup : deve avere cadenza almeno settimanale, l'utilità di backup consente di creare una copia duplicata di tutti i dati presenti nel disco rigido e di archiviare tale copia in un'altra periferica di memorizzazione, ad esempio un disco rigido o un nastro. Se i dati originali presenti nel disco rigido vengono accidentalmente eliminati o sovrascritti, oppure se non è più possibile accedervi a causa di un problema di funzionamento del disco rigido è possibile ripristinarli in modo semplice dal disco o dalla copia archiviata mediante il ripristino guidato. I supporti di backup devono essere custoditi in locali sicuri.

Disaster Recovery: è obbligatorio soltanto per i titolari che trattano, con strumenti elettronici (PC) i dati sensibili o giudiziari dei propri clienti (studi medici, agenzie di assicurazione, commercialisti, avvocati, ecc...). Il Titolare deve disporre di un sistema e di una procedura scritta che garantisca il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi e non superiori a sette giorni. Il Titolare è inoltre obbligato ad effettuare almeno un test di ripristino all'anno (di cui deve conservare la documentazione per gli eventuali controlli) e a pianificare, di anno in anno, la data del test successivo.

Tutti coloro che utilizzano, per la propria attività, almeno un PC

13	Amministratore di sistema	<p>Sono soggetti ai nuovi adempimenti relativi all'amministratore di sistema tutti i titolari che:</p> <ul style="list-style-type: none">a) dispongono di almeno di un amministratore di sistema interno diverso dal Legale rappresentante;b) trattano con strumenti elettronici i dati sensibili o giudiziari dei propri clienti oppure (studi medici, agenzie di assicurazione, commercialisti, avvocati, ecc...) <u>oppure</u> titolari con almeno 250 dipendenti e con un fatturato annuo non inferiore ai 50 milioni di euro.
----	---------------------------	---