

Chek list Privacy PMI

D.lgs. 30/6/2003, n. 196 "Codice in materia di Protezione dei Dati Personali"
All. Del. Gar. N° 21 del 24/5/2007



info@gmtconsulting.net
www.gmtconsulting.net

La seguente lista di controllo è tratta dall'allegato alla Delibera del Garante per la protezione dei dati personali n° 21, del 24/5/2007, recante misure per la semplificazione per le Piccole e Medie imprese.

La check list tiene quindi già conto di tutte le agevolazioni previste per le PMI.

Per l'interpretazione delle domande, e la consultazione dei requisiti normativi, occorre fare riferimento al D.lgs. 30 giugno 2003, n. 196 "Codice in materia di Protezione dei Dati Personali"

Citiamo per comodità Le definizioni di cui all'art. 4 del Codice, che spiegano cosa deve intendersi per "dato personale" e "trattamento":

Art. 4. Definizioni

1. Ai fini del presente codice si intende per:

- a) "trattamento", qualunque operazione** o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- b) "dato personale", qualunque informazione** relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

La risposta negativa ad uno dei seguenti quesiti, denota un possibile profilo critico dal punto di vista della protezione dei dati personali, e richiede un approfondimento, per verificare se si è in regola con il rispetto della normativa.

Quesiti

1	È stata effettuata una valutazione circa le operazioni di trattamento di dati personali, anche sensibili, effettuate dall'impresa?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
2	I dati trattati sono pertinenti e non eccedenti rispetto alle legittime finalità del trattamento, oltre che esatti e aggiornati?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
3	Le persone fisiche che all'interno dell'impresa trattano dati personali sono state designate tutte quali "incaricate del trattamento"?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
4	Sono state fornite a tutti gli "incaricati del trattamento" istruzioni scritte circa i propri compiti?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
5	Se all'interno dell'impresa sono stati individuati soggetti che hanno ambiti di autonomia nel trattamento dei dati personali, sono stati designati per iscritto "responsabili del trattamento"?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
6	Se fuori dell'impresa enti o persone fisiche trattano dati personali nel suo interesse, obbligati a seguirne le istruzioni (come accade per i casi di outsourcing), sono stati designati per iscritto quali "responsabili del trattamento"?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
7	Si è verificato, prima di intraprendere operazioni di trattamento, se l'impresa effettua i trattamenti da notificare al Garante?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>

Chek list Privacy PMI

D.lgs. 30/6/2003, n. 196 "Codice in materia di Protezione dei Dati Personali"
All. Del. Gar. N° 21 del 24/5/2007



info@gmtconsulting.net
www.gmtconsulting.net

8	Se sono intervenute modificazioni relativamente ai trattamenti già eventualmente notificati, è stato curato il loro aggiornamento in una nuova notificazione?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
9	Se cessano i trattamenti, ciò ha formato oggetto di specifica notificazione?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
10	È stata fornita l'informativa agli interessati in caso di dati raccolti presso di essi?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
11	È stata fornita l'informativa agli interessati in caso di dati raccolti presso soggetti diversi dagli interessati	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
12	Il trattamento dei dati personali viene effettuato in presenza di uno dei presupposti di liceità indicati all'art. 24 del Codice?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
13	Se non ricorre uno dei presupposti di liceità indicati all'art. 24 del Codice, è stato raccolto il consenso dell'interessato?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
14	Se sono trattati dati sensibili è stato raccolto il consenso scritto degli interessati?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
15	Se sono trattati dati sensibili, è stato verificato se il trattamento rientra tra quelli già autorizzati dal Garante con le autorizzazioni generali?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
16	Se il trattamento di dati sensibili non rientra tra quelli previsti dalle autorizzazioni generali, è stata richiesta al Garante un'autorizzazione <i>ad hoc</i> ?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
17	Sono state adottate idonee misure di sicurezza per proteggere i dati personali?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
18	Sono state adottate le misure minime di sicurezza previste dal Codice per proteggere i dati personali?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
19	Se sono trattati dati sensibili e giudiziari, è stato redatto, quando è necessario, il documento programmatico per la sicurezza (DPS) e ne vengono osservate le previsioni?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
20	Periodicamente, e comunque entro il 31 marzo di ciascun anno, formano oggetto di rinnovata valutazione le misure di sicurezza individuate con il documento programmatico per la sicurezza (DPS)?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
21	Se i dati personali trattati dall'impresa sono soggetti a trasferimento verso Paesi terzi (esterni all'Unione europea e all'area economica europea), il trasferimento avviene: • in presenza di una delle condizioni previste dall'art. 43 del Codice? oppure • verso uno dei paesi che assicurano un livello adeguato di protezione (Svizzera, Argentina, Isola di Man, Baliato di Guernsey)? oppure • verso un'impresa statunitense che aderisce al <i>Safe Harbor</i> ? oppure • in presenza di clausole contrattuali <i>standard</i> tra esportatore e importatore? oppure • in presenza di un'autorizzazione <i>ad hoc</i> da parte del Garante?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>
22	In presenza dell'esercizio del diritto d'accesso, viene dato riscontro all'interessato secondo le modalità previste dalla legge?	SI	<input type="checkbox"/>
		NO	<input type="checkbox"/>

Chek list Privacy PMI

D.lgs. 30/6/2003, n. 196 "Codice in materia di Protezione dei Dati Personali"
All. Del. Gar. N° 21 del 24/5/2007



Sanzioni **(Violazioni amministrative e Illeciti penali)** (Titolo III, D.lgs. 30 giugno 2003, n. 196)

Capo I - Violazioni amministrative

Art. 161. Omessa o inidonea informativa all'interessato

1. La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma **da seimila euro a trentaseimila euro**.

Art. 162. Altre fattispecie

1. La cessione dei dati in violazione di quanto previsto dall'articolo 16, comma 1, lettera b), o di altre disposizioni in materia di disciplina del trattamento dei dati personali è punita con la sanzione amministrativa del pagamento di una somma **da diecimila euro a sessantamila euro**.

2. (24) La violazione della disposizione di cui all'articolo 84, comma 1, è punita con la sanzione amministrativa del pagamento di una somma **da mille euro a seimila euro**.

2-bis. (25) In caso di trattamento di dati personali effettuato in violazione delle misure indicate nell'articolo 33 o delle disposizioni indicate nell'articolo 167 è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma **da diecimila euro (26) a centoventimila euro**. Nei casi di cui all'articolo 33 è escluso il pagamento in misura ridotta.

2-ter. (26) In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'articolo 154, comma 1, lettere c) e d), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma **da trentamila euro a centottantamila euro**.

2-quater. (27) La violazione del diritto di opposizione nelle forme previste dall'articolo 130, comma 3-bis, e dal relativo regolamento è sanzionata ai sensi del comma 2-bis del presente articolo.

Art. 162-bis. Sanzioni in materia di conservazione dei dati di traffico (28)

1. Salvo che il fatto costituisca reato e salvo quanto previsto dall'articolo 5, comma 2, del decreto legislativo di recepimento della direttiva 2006/24/Ce del Parlamento europeo e del Consiglio del 15 marzo 2006, nel caso di violazione delle disposizioni di cui all'art. 132, commi 1 e 1-bis, si applica la sanzione amministrativa pecuniaria da 10.000 euro a 50.000 euro (29).

Art. 163. Omessa o incompleta notificazione

1. (30) Chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione ai sensi degli articoli 37 e 38, ovvero indica in essa notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma **da ventimila euro a centoventimila euro**.

Art. 164. Omessa informazione o esibizione al Garante

1. (31) Chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli articoli 150, comma 2, e 157 è punito con la sanzione amministrativa del pagamento di una somma **da diecimila euro a sessantamila euro**.

Art. 164-bis. Casi di minore gravità e ipotesi aggravate (32)

1. Se taluna delle violazioni di cui agli articoli 161, 162, 163 e 164 è di minore gravità, avuto altresì riguardo alla natura anche economica o sociale dell'attività svolta, i limiti minimi e massimi stabiliti dai medesimi articoli sono applicati in misura pari a due quinti.

2. In caso di più violazioni di un'unica o di più disposizioni di cui al presente Capo, a eccezione di quelle previste dagli articoli 162, comma 2, 162-bis e 164, commesse anche in tempi diversi in relazione a banche di dati di particolare rilevanza o dimensioni, si applica la sanzione amministrativa del pagamento di una somma **da cinquantamila euro a trecentomila euro**. Non è ammesso il pagamento in misura ridotta.

3. In altri casi di maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi interessati, i limiti minimo e massimo delle sanzioni di cui al presente Capo sono applicati in misura pari al doppio.

4. Le sanzioni di cui al presente Capo possono essere aumentate fino al quadruplo quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore.

Art. 165. Pubblicazione del provvedimento del Garante

1. (33) Nei casi di cui agli articoli del presente Capo può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica. La pubblicazione ha luogo a cura e spese del contravventore.

Art. 166. Procedimento di applicazione

1. L'organo competente a ricevere il rapporto e ad irrogare le sanzioni di cui al presente capo e all'articolo 179, comma 3, è il Garante. Si osservano, in quanto applicabili, le disposizioni della legge 24 novembre 1981, n. 689, e successive modificazioni. I proventi, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'articolo 156, comma 10, e sono utilizzati unicamente per l'esercizio dei compiti di cui agli articoli 154, comma 1, lettera h), e 158.

Capo II - Illeciti penali

Art. 167. Trattamento illecito di dati

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva documento, con la **reclusione da sei a diciotto mesi** o, se il fatto consiste nella comunicazione o diffusione, con la **reclusione da sei a ventiquattro mesi**.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva documento, con la **reclusione da uno a tre anni**.

Art. 168. Falsità nelle dichiarazioni e notificazioni al Garante

1. Chiunque, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la **reclusione da sei mesi a tre anni**.

Art. 169. Misure di sicurezza

1. (34) Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'**arresto sino a due anni**.

2. (35) All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per

Chek list Privacy PMI

D.lgs. 30/6/2003, n. 196 "Codice in materia di Protezione dei Dati Personali"
All. Del. Gar. N° 21 del 24/5/2007



l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.

Art. 170. Inosservanza di provvedimenti del Garante

1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la **reclusione da tre mesi a due anni**.

Art. 171. Altre fattispecie

1. La violazione delle disposizioni di cui agli articoli 113, comma 1, e 114 è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300.

Art. 172. Pene accessorie

1. La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza.