ELENCO DEGLI ADEMPIMENTI RICHIESTI A TITOLARI DEL TRATTAMENTO PRIVATI DALLA NORMATIVA PRIVACY.

Il presente documento ha lo scopo di illustrare gli adempimenti di natura legale e di natura tecnico-informatica in materia di privacy che devono essere adottati dai titolari del trattamento privati al fine di rispettare pienamente tutti i vincoli normativi previsti dal decreto legislativo 30 Giugno 2003, n. 196 (di seguito anche "Codice della privacy" o "Codice") e sanzionati – in ipotesi di violazione – sia sul piano civile, che su quello amministrativo e soprattutto penale.

Adempimenti organizzativi di natura legale e di carattere generale.

A titolo esemplificativo, ogni titolare del trattamento è tenuto:

(a) a verificare se sia o meno obbligatoria per i trattamenti di dati personali svolti la effettuazione della **notificazione telematica** dei trattamenti di dati personali all'Autorità Garante (la notificazione è oggi obbligatoria solo per peculiari tipologie di trattamenti di dati personali e per alcune categorie di dati, come ad esempio i dati genetici, i dati biometrici, i dati sanitari o sulla vita sessuale trattati nell'ambito della prestazione di servizi sanitari per via telematica, etc);

(b) alla nomina di uno o più Responsabili del trattamento (nomina comunque solo facoltativa, in caso il titolare non vi proceda le "responsabilità" saranno esclusivamente in capo al titolare del trattamento, cioè in capo all'azienda in quanto tale e non in capo alle persone fisiche che la rappresentano, tipo CDA, presidente, AD, etc);

(c) alla nomina degli incaricati del trattamento (nomina invece obbligatoria che riguarda le sole persone fisiche – interne all'azienda o esterne - che trattano dati personali su istruzioni del Responsabile o del Titolare e che devono ricevere specifiche istruzioni per iscritto. E' possibile effettuare nomine singole e nominative o nomine per classi omogenee di incaricati tutti addetti ad una specifica unità produttiva);

(d) al rilascio delle informative ai sensi dell'art. 13 del Codice della privacy nei confronti di qualsiasi interessato, ora rappresentato solo da persone fisiche cui si riferiscono i dati personali (dipendenti, collaboratori, clienti, fornitori, etc), essendo stata introdotta l'inapplicabilità del Codice della privacy ai dati delle persone giuridiche a far data dal d.l. 6 Dicembre 2011, n. 201 poi convertito in legge;

(e) ad acquisire il consenso al trattamento dei dati da parte degli interessati, nei casi in cui ciò sia obbligatorio (per i trattamenti di dati sensibili in forma scritta o equivalente) come ad es. per finalità di marketing o proflazione;

(f) a rispettare le specifiche prescrizioni organizzative e gestionali previste per i casi di trattamenti di dati sensibili o giudiziari dalle applicabili **Autorizzazioni Generali al trattamento dei dati sensibili o giudiziari** emanate dal Garante (in tutto sono 7 Autorizzazioni generali – applicabili a seconda dei casi – più la recente Autorizzazione Generale al trattamento dei dati genetici);

(g) ad implementare corrette politiche di trattamento **quando i dati sono trasferiti all'estero in Paesi non appartenenti all'Unione Europea**, adeguandosi o alle Autorizzazioni Generali sul trasferimento all'estero dei dati personali o implementando le specifiche misure previste in materia dagli articoli 43-46 del Codice della privacy);

(h) ad adeguare i trattamenti di dati personali rappresentati da **immagini riprese e/o conservate mediante impianti di videosorveglianza** sia esterni che interni ai locali dell'ente (ove tali trattamenti siano svolti) ai sensi del Provvedimento Generale sulla Videosorveglianza emanato dal Garante l'8 Aprile 2010 (che sostituisce il precedente del Aprile 2004).

Adempimenti organizzativi di natura legale e di carattere specifico.

I titolari del trattamento devono tenere presente che – al di là delle norme contenute nel Codice della privacy, nei codici di deontologia e buona condotta sul trattamento dei dati personali in particolari settori o nelle Autorizzazioni Generali sul trattamento dei dati sensibili o giudiziari - vi sono numerosi **Provvedimenti Generali** che l'Autorità Garante ha emanato nel corso del tempo e che è obbligatorio rispettare e implementare, pena sanzioni assai elevate.

Tra i Provvedimenti Generali (oltre a quello sulla videosorveglianza già richiamato) che interessano la gran parte dei titolari, si citano a solo titolo esemplificativo i seguenti:

- le "***Linee guida in materia di trattamento di dati personali di lavoratori alle dipendenze di datori di lavoro privati***" (Deliberazione 53/2006);
- le ***Linee Guida per email e Internet*** (Deliberazione 13/2007), che prevedono la redazione del Disciplinare Interno sull'utilizzo di email e Internet da parte dei lavoratori;
- il Provvedimento del Garante del 15 giugno 2011 "***Titolarità del trattamento di dati personali in capo ai soggetti che si avvalgono di agenti per attività promozionali***" (adempimento entro il 30 Novembre 2011);
- il Provvedimento Generale sulla nomina degli Amministratori di Sistema "***Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema***" (da implementarsi entro il 30 Giugno 2009);

- il Provvedimento 21 Luglio 2011 "***Trattamento di dati personali nell'ambito della una selezione del personale";***
- il Provvedimento 19 Gennaio 2011 "***Prescrizioni per il trattamento di dati personali per finalita' di marketing, mediante l'impiego del telefono con operatore, a seguito dell'istituzione del registro pubblico delle opposizioni* "**.

Infine, tra gli adempimenti organizzativi di natura legale di carattere specifico vi è anche l'esigenza per ogni titolare del trattamento di adeguare la raccolta e il trattamento dei dati personali on-line (ad esempio mediante il sito web ufficiale).

L'elencazione di cui sopra è esemplificativa. Gli adeguamenti richiesti possono altresì riguardare, in base ad ulteriori e diversi Provvedimenti Generali del Garante, la conformità delle politiche di trattamento dei dati a prescrizioni specifiche applicabili a diverse categorie di titolari del trattamento pubblici o privati.


Adeguamento delle misure di sicurezza da adottare nel trattamento di dati personali.

Una corretto adeguamento dei trattamenti di dati personali al Codice della Privacy non può ovviamente prescindere dall'importante tematica - sia di tipo **legale** che, soprattutto, di tipo **tecnico-informatico** – della adozione delle misure idonee o minime di sicurezza nel trattamento richiesta dagli artt. da 31 a 36 del Codice e dal Disciplinare Tecnico sulle Misure Minime di Sicurezza – Allegato B al Codice.

Difatti, pur avendo il d.l. 9 febbraio 2012, n. 5 - convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35 - abrogato l'obbligo di adottare ed aggiornare annualmente il **Documento Programmatico sulla Sicurezza**, **non sono venuti meno gli obblighi di implementare le altre misure di sicurezza** che il DPS – solo una della misure - complessivamente documentava (in sostanza, è venuto meno l'obbligo di documentare nello specifico, ma non quello di adottare le altre misure).

Il trattamento di dati personali **effettuato con strumenti elettronici** è difatti consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico (Allegato B al Codice della privacy) le seguenti **misure minime obbligatorie**:

(a) autenticazione informatica;

(b) adozione di procedure di gestione delle credenziali di autenticazione;

(c) utilizzazione di un sistema di autorizzazione;

(d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

(e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

(f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

(g) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Il trattamento di dati personali effettuato **senza l'ausilio di strumenti elettronici** è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico (Allegato B al Codice della privacy) le seguenti misure minime:

(a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati;

(b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

(c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Si ricorda infine che per taluni trattamenti particolari (ad esempio il trattamento di dati genetici) oltre alle misure minime di sicurezza devono essere adottate anche ulteriori misure idonee, o contenute nell'Autorizzazione Generale del Garante sul trattamento dei dati genetici o comunque appropriate alla natura ed ai rischi connessi ai trattamenti (in questo caso l'idoneità della misura di sicurezza nel trattamento dei dati genetici varia a seconda dei casi e delle attività dell'azienda).

* * *

Il processo che conduce alla corretta adozione delle misure di sicurezza per la protezione dei dati personali, in particolare per quanto riguarda quelle minime obbligatorie, deve svolgersi attraverso una serie di fasi che viene descritta sinteticamente nei punti successivi.

Le fasi che – esemplificativamente – ciascun titolare dovrebbe prevedere sono le seguenti:

Inventario dei sistemi informatici	Realizzare un inventario dei sistemi informatici esistenti, avente lo scopo di fornire un quadro di riferimento sintetico ma qualificante della struttura tecnologica esistente. In particolare dovrebbero essere documentati: ▪ I server ed i sistemi gestionali esistenti ▪ I client (per classi) ▪ Le reti aziendali ▪ Le connessioni con l'ambiente esterno ▪ Le applicazioni utilizzate per il trattamento dei dati personali

Individuazione dei profili di autorizzazione	Dovrebbe essere documentato l'accesso alle applicazioni da parte dei gruppi omogenei di incaricati, che devono essere documentate e verificate con periodicità almeno annuale
Documentazione della protezione mediante backup dei dati personali	Dovrebbero essere inventariati i dispositivi di backup esistenti; individuati gli archivi dei quali viene effettuato il salvataggio su ogni dispositivo, documentate le modalità tecniche ed organizzative di esecuzione dei salvataggi
Documentazione della protezione mediante sistemi antivirus	Dovrebbe essere documentata la presenza di software di protezione su tutti i sistemi di elaborazione, nonché le modalità per garantirne l'aggiornamento
Documentazione della protezione da intrusioni (sistemi di firewall)	Dovrebbero essere descritti i sistemi di firewall per le comunicazioni con l'esterno soggette a rischio di intrusione

Documentazione delle misure di protezione logistica	Dovrebbero essere descritti gli strumenti e le procedure che forniscono una protezione logistica ed ambientale (ad es. sistemi di limitazione degli accessi, sistemi di protezione dagli incendi), sia di tipo generale applicati all'intera azienda, sia specifici applicati ai sistemi di elaborazione
Analisi dei rischi	L'analisi dei rischi dovrebbe essere condotta mediante la predisposizione di una tabella riassuntiva riportante tutti i rischi individuati, con la valutazione del livello di rischio relativo, e l'insieme delle contromisure poste in essere o di prevedibile adozione. L'analisi dovrebbe essere condotta mediante la verifica di un insieme predefinito e categorizzato di rischi e di contromisure, che può essere implementato per adattarlo alla specifica realtà dell'azienda.

Documentazione del piano di formazione agli incaricati del trattamento	Dovrebbe essere documentato il progetto formativo, individuando per ogni categoria si incaricati, contenuti e modalità di formazione in rapporto alla rilevanza dei relativi ambiti di trattamento ed all'utilizzo dei sistemi informatici
Nomina degli amministratori di sistema	Dovrebbero essere predisposte le misure gestionali e organizzative di cui al provvedimento del Garante 27 Novembre 2008 " *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"*

Incremento degli importi a titolo di sanzioni amministrative per violazione del Codice della privacy.

Per utilità, si ricorda che con decreto-legge del 30 Dicembre 2008, n. 207 sono state introdotte assai rilevanti modifiche all'impianto sanzionatorio/amministrativo del Codice della privacy. Le sanzioni amministrative in caso di violazione delle regole sul trattamento dei dati personali sono state aumentate in maniera assai rilevante.

Si ricorda che oltre alle sanzioni amministrative, il Codice della privacy prevede altresì sanzioni di natura penale (per il reato di "Illecito trattamento dei dati personali" di cui all'art. 167 del Codice della privacy) e rimedi di natura civilistica esperibili dagli interessati (risarcimento del danno da trattamento dei dati personali ai sensi dell'art. 15 del Codice della privacy).

Di seguito le principali sanzioni per violazioni amministrative.

Omessa o inidonea informativa sul trattamento dei dati personali (art. 161 Codice privacy)

Sanzione **da 6 a 36 mila Euro** per l'omessa o inidonea informativa sul trattamento dei di dati personali, con possibile aumento della sanzione fino al quadruplo.

Violazione degli obblighi in materia di misure minime di sicurezza (art. 162 Codice privacy).

Sanzione **da ventimila euro a centoventimila euro**

Inosservanza dei provvedimenti del Garante (art. 162 Codice privacy)

Sanzione **da trentamila euro a centottantamila euro**.

Omessa o incompleta notificazione dei trattamenti al Garante (art. 163 Codice privacy)

Sanzione **da 20 mila Euro a 120 mila Euro**.

Omessa adozione di misure di sicurezza (art. 169 Codice privacy).

Arresto fino a due anni o oblazione pari a **30 mila euro**.

Violazione dell'ordine del Garante di fornire informazioni e/o di esibire documenti (art. 164 Codice privacy).

Sanzione **da 10 a 60 mila Euro**

Cessione dei dati in violazione della disciplina rilevante.

Sanzione da **10 a 60 mila euro.**

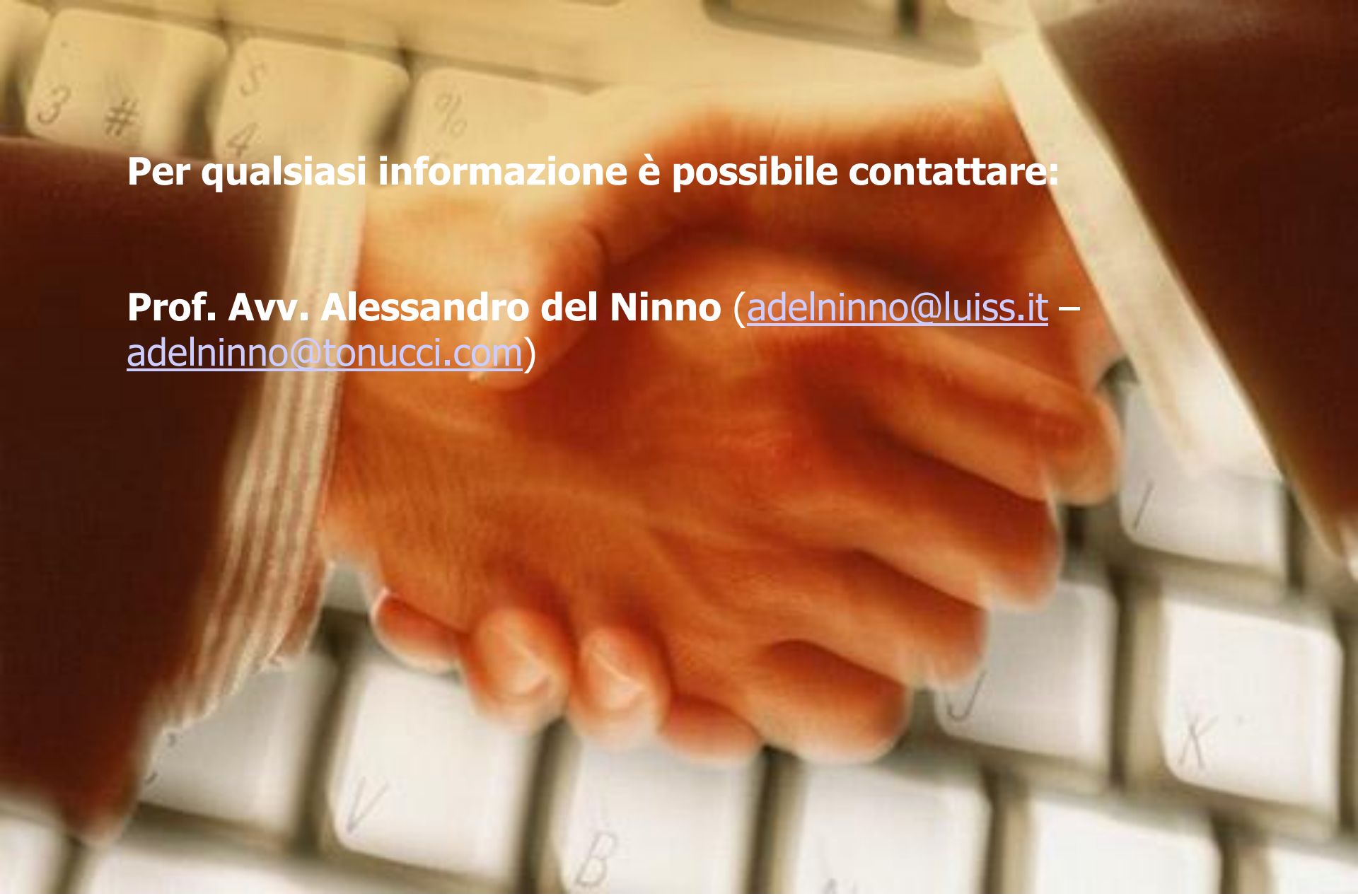
Comunicazione di dati sanitari non attraverso personale medico (art. 84 Codice privacy).

Sanzione **da mille a seimila euro**.

Violazione dell'art. 162-bis in materia di data retention (applicabile solo a fornitori di servizi di comunicazione elettronica).

Sanzione **da 10 a 50 mila euro**

Le sanzioni – a seconda dei casi – possono essere diminuite dei 2/5 (in casi di minore gravità) o aumentate del quadruplo (nei casi di maggiore gravità).



Per qualsiasi informazione è possibile contattare:

Prof. Avv. Alessandro del Ninno (adelninno@luiss.it – adelninno@tonucci.com)