

## Giudizio di conformità sugli adempimenti richiesti

<b>Obiettivi di controllo</b>	<b>Presidio</b>	<b>Verifica effettuata</b>	<b>Grado di conformità</b>
<u>Censimento dei trattamenti</u>			
Tutti i trattamenti di dati personali effettuati (anche in parte) mediante strumenti elettronici sono censiti e sono indicati i relativi "amministratori di sistema".	Il regolamento aziendale XX prevede che l'inizio di qualsiasi nuovo trattamento di dati personali sia comunicato al responsabile aziendale della privacy che provvede ad aggiornare il censimento dei trattamenti	È stata presa visione dell'ultimo censimento dei trattamenti disponibile presso il responsabile aziendale della privacy e verificato che fosse completo.	1) Conforme ____ 2) Non conforme ____ 3) Parzialmente conforme ____ 4) Non applicabile ____ Note (per 3 o 4):
Se i trattamenti sono affidati a terze parti queste hanno comunicato al Titolare l'elenco dei relativi "amministratori di sistema".	Nei contratti di outsourcing sono inserite clausole specifiche a riguardo. Almeno una volta l'anno viene richiesto l'aggiornamento della lista degli amministratori di sistema	È stata presa visione degli elenchi forniti dagli <i>outsourcer</i> .	1) Conforme ____ 2) Non conforme ____ 3) Parzialmente conforme ____ 4) Non applicabile ____ Note (per 3 o 4):
Se il trattamento comprende, "anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori" è stata resa nota e conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni.	L'informativa ai dipendenti prevede tale comunicazione. L'ufficio Formazione cura attraverso la intranet aziendale gli aggiornamenti al personale relativi a tale adempimento.	È stata presa visione delle lettere di incarico. È stata consultata la intranet per verificare la presenza di tali comunicazioni.	1) Conforme ____ 2) Non conforme ____ 3) Parzialmente conforme ____ 4) Non applicabile ____ Note (per 3 o 4):
<u>Lettera di incarico</u>			
Per ogni "amministratore di sistema" è	Esiste uno standard di lettera di incarico	È stata acquisita copia dello standard.	

disponibile la lettera di incarico comprendente (al minimo):	ad "amministratore di sistema" che prevede le caratteristiche richieste dalla legge.		
<ul style="list-style-type: none"> <li>• attestazione che l'incaricato ha le caratteristiche richieste dalla legge;</li> </ul>			
<ul style="list-style-type: none"> <li>• elencazione analitica degli ambiti di operatività richiesti e consentiti in base al profilo di autorizzazione assegnato;</li> </ul>			1) Conforme _____ 2) Non conforme ____ 3) Parzialmente conforme _____ 4) Non applicabile ____ Note (per 3 o 4):
<ul style="list-style-type: none"> <li>• indicazione delle "verifiche" almeno annuali che il titolare svolgerà sulle attività svolte dall'amministratore di sistema;</li> </ul>			1) Conforme _____ 2) Non conforme ____ 3) Parzialmente conforme _____ 4) Non applicabile ____ Note (per 3 o 4):
<ul style="list-style-type: none"> <li>• indicazione che la nomina ed il relativo nominativo sarà comunicato al personale ed eventualmente a terzi nei modi richiesti dalla legge.</li> </ul>			1) Conforme _____ 2) Non conforme ____ 3) Parzialmente conforme _____ 4) Non applicabile ____ Note (per 3 o 4):
<u>Elenco degli amministratori</u>			
Gli estremi identificativi delle persone fisiche nominate "amministratori di sistema", con l'elenco delle funzioni ad essi attribuite, sono stati riportati nel Documento Programmatico sulla Sicurezza, oppure, nei casi in cui il	È stato predisposto un "elenco degli amministratori" ed allegato al Documento Programmatico sulla Sicurezza.	È stato acquisito il DPS e l'allegato relativo all'elenco degli amministratori	1) Conforme _____ 2) Non conforme ____ 3) Parzialmente conforme _____ 4) Non applicabile ____ Note (per 3 o 4):

titolare non sia tenuto a redigerlo, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.			
<u>Registrazione degli accessi</u>			
È adottato un idoneo sistema per la registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema.	In azienda è in uso il <b>sistema ABC</b> di gestione degli accessi logici; tale sistema prevede il log degli accessi.	È stata presa visione del sistema ABC e del manuale che ne descrive le caratteristiche	1) Conforme _____ 2) Non conforme ____ 3) Parzialmente conforme _____ 4) Non applicabile ____  Note (per 3 o 4):
Tali registrazioni ( <i>access log</i> ) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.	Il log degli accessi relativi agli amministratori di sistema è protetto con credenziali specifiche che sono custodite dal Direttore Generale in busta sigillata dentro una cassaforte. Il DG non è a conoscenza delle credenziali. In caso di necessità le credenziali sono date in uso al personale tecnico e poi modificate e nuovamente assegnate al Direttore Generale. Il <b>sistema ABC</b> di gestione dei log mantiene copia inalterabile dei log.	È stata presa visione delle credenziali riservate custodite dal Direttore Generale. È stata presa visione del sistema ABC e del manuale che ne descrive le caratteristiche.	1) Conforme _____ 2) Non conforme ____ 3) Parzialmente conforme _____ 4) Non applicabile ____  Note (per 3 o 4): _____
Le registrazioni comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate e sono conservate per un congruo periodo, non inferiore a sei mesi.	I log sono conservati per sei mesi.	Sono stati visionati i log.	1) Conforme _____ 2) Non conforme ____ 3) Parzialmente conforme _____ 4) Non applicabile ____  Note (per 3 o 4):

<u>Verifiche del titolare</u>			
L'operato degli amministratori di sistema è verificato, con cadenza almeno annuale, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.	Annualmente, in occasione dell'aggiornamento del Documento Programmatico sulla Sicurezza, viene verificato il rispetto degli obblighi normativi relativi all'amministratore di sistema.	È stata compilata la presente check list in occasione dell'aggiornamento del DPS:	1) Conforme _____ 2) Non conforme ____ 3) Parzialmente conforme _____ 4) Non applicabile ____  Note (per 3 o 4):
Per i trattamenti affidati a terze parti, queste hanno attestato per iscritto di aver effettuato, con cadenza almeno annuale, le verifiche sui relativi amministratori di sistema in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.	Annualmente, in occasione dell'aggiornamento del Documento Programmatico sulla Sicurezza, viene richiesta alle terze parti che hanno in <i>outsourcing</i> trattamenti di dati personali dell'azienda, l'attestazione sulle verifiche del rispetto degli obblighi normativi relativi all'amministratore di sistema.	Sono state visionate le attestazioni da parte degli <i>outsourcer</i> .	1) Conforme _____ 2) Non conforme ____ 3) Parzialmente conforme _____ 4) Non applicabile ____  Note (per 3 o 4): _____

## Valutazione dei possibili rischi (e relativi impatti)

<i>Obiettivi di controllo</i>	<i>Grado di conformità</i>	<i>Note sul grado di conformità</i>	<i>Rischi</i>	<i>Impatti</i>
<u>Censimento dei trattamenti</u>	Conforme			
<u>Lettera di incarico</u>	Conforme			
<u>Elenco degli amministratori</u>	Parzialmente conforme	Mancano le liste relative a due società terze nominate responsabili del trattamento.	Rischio di accesso non autorizzato Rischio di trattamento non consentito o non conforme alle finalità della raccolta	sanzione da 20.000 a 120.000 euro
<u>Registrazione degli accessi</u>	Parzialmente conforme	Tecnicamente non si ha evidenza del fatto che i log non siano effettivamente modificabili.	Rischio di distruzione o perdita, anche accidentale, dei dati Rischio di accesso non autorizzato Rischio di trattamento non consentito o non conforme alle finalità della raccolta	sanzione da 20.000 a 120.000 euro
<u>Verifiche del titolare</u>	Parzialmente conforme	Non esistono piani di formazione volti ad un costante aggiornamento degli amministratori di sistema in relazione agli adempimenti di legge.	Mancata adozione di misure minime di sicurezza	sanzione da 20.000 a 120.000 euro

**Indicazioni dei possibili interventi (se necessari o opportuni)**

<i>Obiettivi di controllo</i>	<i>Note sul grado di conformità</i>	<i>Azione</i>	<i>Data di completamento</i>	<i>In carico a</i>
<u>Elenco degli amministratori</u>	Mancano le liste relative a due società terze nominate responsabili del trattamento.	Ottenere le liste mancanti. Disdire il contratto in mancanza delle liste entro 30 giorni.	1 giugno 2009	Ufficio Legale
<u>Registrazione degli accessi</u>	Tecnicamente non si ha evidenza del fatto che i log non siano effettivamente modificabili	Individuare una soluzione che garantisca l'immodificabilità dei log.	30 luglio 2009	Sistemi informativi
<u>Verifiche del titolare</u>	Non esistono piani di formazione volti ad un costante aggiornamento degli amministratori di sistema in relazione agli adempimenti di legge	Aggiornare il piano di formazione degli amministratori di sistema.	15 aprile 2009	Ufficio Formazione