

# MODELLO DI APA2012

## AGGIORNAMENTO PRIVACY ANNUALE<sup>123</sup>

AGGIORNATO AL .....

### PUNTO N°1

#### DATI PERSONALI TRATTATI

Le categorie di dati personali trattati dal Titolare sono le seguenti (*a titolo meramente esemplificativo si riporta quanto segue*):

- **A1:** dati comuni relativi a Fornitori
- **A2:** dati comuni relativi ai Clienti
- **A3:** dati comuni relativi ai potenziali Clienti
- **A4:** dati relativi a Candidati da considerare per l'instaurazione di un rapporto di lavoro di natura anche sensibile
- **A5:** dati comuni relativi agli utenti dei servizi online
- **A6:** dati particolari relativi a terzi ripresi dal sistema di videosorveglianza
- **A7:** .....

I dati personali trattati dal Titolare sono i seguenti:

- **T1:** Fatture e corrispondenza dei *propri fornitori*, con indicazione sulle stesse dei dati fiscali e civilistici obbligatori per legge volti ad individuare i soggetti fra i quali è intercorso un rapporto giuridico o economico;
- **T2:** Dati comuni necessari all'adempimento degli obblighi di legge e contrattuali, fatture e corrispondenza della *propria clientela*, con indicazione sulle stesse dei dati fiscali e civilistici obbligatori per legge volti ad individuare i soggetti fra i quali è intercorso un rapporto giuridico o economico;
- **T3:** Dati comuni *relativi ai Potenziali clienti* necessari a sviluppare futuri rapporti commerciali;
- **T4:** Dati personali di *candidati* finalizzati all'eventuale instaurazione di un rapporto di lavoro subordinato, tra i quali ve ne possono essere taluni di natura sensibile;

---

<sup>1</sup> **Note Legali per l'Uso del Modello di Aggiornamento Privacy Annuale.** La e l'elaborazione del presente Modello di Aggiornamento Privacy Annuale, anche se curato con scrupolosa attenzione, non può comportare specifiche responsabilità per eventuali involontari errori, inesattezze o uso scorretto. Sono consentite citazioni a titolo di cronaca, studio, critica o recensione, purché accompagnate dall'indicazione della fonte. Il presente facsimile si riferisce alla normativa vigente al momento in cui è stato predisposto (6 marzo 2012). Si invita pertanto il lettore a porre la massima attenzione alla data ed eventualmente documentarsi circa possibili successive modifiche legislative.

L'Autore ha compiuto ogni ragionevole sforzo per assicurare che il Modello fosse attentamente vagliato ed analizzato, oltre che elaborato con la massima cura e aggiornato. Tuttavia errori, inesattezze ed omissioni sono sempre possibili. Si declina, pertanto, qualsiasi responsabilità per errori, inesattezze ed omissioni eventualmente presenti nel testo del presente Modello.

Nessuna responsabilità viene assunta in relazione all'uso che terzi potrebbero fare del contenuto di quanto inserito nel presente Modello. L'Autore, pertanto, non sarà tenuto a rispondere in ordine a danni, perdite, pregiudizi di alcun genere che terzi potranno subire a seguito dell'uso del presente Modello di Aggiornamento Privacy Annuale.

<sup>2</sup> Almeno annualmente, ogni Titolare deve:

- ✓ Verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione;
- ✓ Aggiornare l'elenco di "chi fa cosa" (Incaricati e Responsabili trattamento);
- ✓ Aggiornare l'Informativa completa e la Privacy Policy sul sito web
- ✓ Verificare le attività degli Amministratori di Sistema: l'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei Titolari del trattamento o dei Responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti;
- ✓ Programmare gli interventi formativi.

<sup>3</sup> V. anche: <http://studiomazzolari.wordpress.com/2012/02/28/dps-addio-benvenuto-apa/>

- **T5:** Dati personali dei *propri dipendenti e collaboratori* indispensabili allo svolgimento del rapporto di lavoro e contrattuale, tra i quali ve ne sono alcuni di natura sensibile (dati dai quali si ricavano informazioni sullo stato di salute o sull'adesione a sindacati);
- **T6:** dati personali degli *utenti del sito web* di natura comune;
- **T7:** immagini *relative a terzi* raccolte attraverso il sistema di videosorveglianza aziendale.
- **T8:** .....

**PUNTO N° 2**

**INCARICATI DEL TRATTAMENTO E UNITÀ ORGANIZZATIVE DI APPARTENENZA<sup>4</sup>**

	U1	U2	U3	U4	....
<b>Unità Organizzativa →</b>	<b>Amministrazione</b>	<b>Risorse Umane</b>	<b>Commerciale</b>	.....	.....
<b>Incaricati del trattamento ↓</b>					
.....	X				
.....		X			
.....			X		
.....				X	
.....					X
.....					
.....					
.....					

<sup>4</sup> Allocare gli Incaricati del trattamento nominati entro la Funzione/Unità organizzativa di appartenenza.

**PUNTO N°4**  
**UNITÀ ORGANIZZATIVE E TRATTAMENTI EFFETTUATI<sup>5</sup>**

Dati personali →	Dipendenti	Clienti	Potenziali Clienti	Fornitori	Candidati Assunzione	Utenti servizi online	.....
Unità Organizzativa ↓							
<b>U1</b> <b>Amministrazione</b>	Comuni e Sensibili	.....	.....	.....	.....	.....	.....
<b>U2</b> <b>Risorse Umane</b>	.....	.....	.....	.....	.....	.....	.....
<b>U3</b> <b>Commerciale</b>	.....	.....	.....	.....	.....	.....	.....
<b>U4</b> .....	.....	.....	.....	.....	.....	.....	.....
<b>U5</b> .....	.....	.....	.....	.....	.....	.....	.....

<sup>5</sup> Indicare a tipologia di dati personali trattata da ciascuna Funzione/Unità organizzativa (Dati comuni, Sensibili, Giudiziari, Particolari...)

**PUNTO N°5**  
**ARCHIVI E BANCHE DATI DI RIFERIMENTO<sup>6</sup>**

*A titolo meramente esemplificativo si riporta quanto segue:*

- **Archivio Amministrazione – D1:** contenente dati relativi al Personale di natura anche sensibile, ai Fornitori di natura comune.  
L'Archivio è costituito da faldoni e raccoglitori dislocati in un armadio a legno chiudibile a chiave sito nell'Ufficio Amministrazione.
- **Archivio .....** – **D3:** .....
- **Archivio .....** – **D4:** .....
- **Archivio .....** – **D5:** .....
- **Database .....** – **D6:** .....
- **Database .....** – **D7:** .....
- **Database .....** – **D8:** .....

---

<sup>6</sup> Elencare e descrivere Archivi e Database cui gli Incaricati possono avere accesso nello svolgimento delle proprie mansioni lavorative.

**PUNTO N°6**

**UNITÀ ORGANIZZATIVE E ARCHIVI / BANCHE DATI DI ACCESSO<sup>7</sup>**

Archivi/Database →	D1	D2	D3	D4	D5	D6
Unità Organizzativa ↓	Archivio Amministrazione	.....	.....	.....	.....	.....
U1 Amministrazione	X					
U2 Risorse Umane						
U3 Commerciale						
U4 .....						
U5 .....						

<sup>7</sup> Con una "X" indicare chi ha accesso a cosa (coerentemente a quanto indicato nelle rispettive "Lettere d'Incarico")

**PUNTO N°7**

**INCARICATI CUSTODIA ARCHIVI AD ACCESSO CONTROLLATO<sup>8</sup>**

<b>Archivi/Database →</b>	<b>D1</b>	<b>D2</b>	<b>D3</b>
<b>Incaricati custodia ↓</b>	<b>Archivio</b>	.....	.....
	<b>Amministrazione</b>		
.....	X		
.....		X	

---

<sup>8</sup> V. Punto 29, Codice in materia di protezione dei dati personali, Allegato B: Disciplinare tecnico in materia di misure minime di sicurezza (Artt. da 33 a 36 del Codice)

**PUNTO N°8**

**RESPONSABILI DEL TRATTAMENTO**

<b>Descrizione sintetica dell'attività</b>	<b>Ambiti di trattamento interessati</b>	<b>Nominativo</b>	<b>Interno/Esterno</b>	<b>Sede</b>	<b>Descrizione dei criteri o degli impegni assunti per l'adozione della misure</b>
Responsabile del trattamento e del Riscontro	Dati del Personale, Clienti, ..... .....	.....	Interno	.....	
Amministratore di sistema software complesso, di rete e apparati di sicurezza	.....	.....	Esterno	.....	Rilascio dichiarazioni di adottare le misure di sicurezza previste dal Codice privacy
Adeguamento/Aggiornamento privacy policy al DLgs 196/2003	Dati comuni Incaricati e Responsabili del trattamento	.....	Esterno	.....	Rilascio dichiarazioni di adottare le misure di sicurezza previste dal Codice privacy
Svolgimento di investigazioni difensive e all'assistenza legale per far valere o difendere in sede giudiziaria un diritto	.....	.....	.....	.....	Rilascio dichiarazioni di adottare le misure di sicurezza previste dal Codice privacy
Adempimenti obbligatori previsti dall'Art. 25 DLgs 81/2008 – TUSL in materia di igiene e	.....	.....	.....	.....	Rilascio dichiarazioni di adottare le misure di sicurezza

sicurezza nei luoghi di lavoro					previste dal Codice privacy
Manutenzione degli impianti di sicurezza e videosorveglianza	.....	.....	.....	.....	Rilascio dichiarazioni di adottare le misure di sicurezza previste dal Codice privacy
Consulenza fiscale in materia di paghe e contributi dei dipendenti	.....	.....	.....	.....	Rilascio dichiarazioni di adottare le misure di sicurezza previste dal Codice privacy
Adempimento degli obblighi fiscali	.....	.....	.....	.....	Rilascio dichiarazioni di adottare le misure di sicurezza previste dal Codice privacy
.....	.....	.....	.....	.....	Rilascio dichiarazioni di adottare le misure di sicurezza previste dal Codice privacy
.....	.....	.....	.....	.....	Rilascio dichiarazioni di adottare le misure di sicurezza previste dal Codice privacy

**PUNTO N°9**  
**AGGIORNAMENTO PRIVACY POLICY**

<b>Obiettivi di controllo: Aggiornamento Privacy Policy</b>	<b>Presidio</b>	<b>Verifica effettuata</b>	<b>Grado di conformità</b>
<p>Informativa Dipendenti e Collaboratori</p>	<p>Il .....<sup>9</sup> verifica annualmente i contenuti dell'Informativa completa rilasciata</p>	<p>E' stata presa visione dell'ultimo censimento dei trattamenti effettuati dall'Azienda, ne è stata verificata la coerenza con i contenuti dell'Informativa ed è stata aggiornata la data riportata sul documento.</p>	<p>√ Conforme ___ √ Non conforme ___ √ Parzialmente conforme ___ √ Non applicabile ___ Note:</p>
<p>Informativa Clienti</p>	<p>Il ..... verifica annualmente i contenuti dell'Informativa completa rilasciata</p>	<p>E' stata presa visione dell'ultimo censimento dei trattamenti effettuati dall'Azienda, ne è stata verificata la coerenza con i contenuti dell'Informativa ed è stata aggiornata la data riportata sul documento.</p>	<p>√ Conforme ___ √ Non conforme ___ √ Parzialmente conforme ___ √ Non applicabile ___ Note:</p>
<p>Informativa Fornitori</p>	<p>Il ..... verifica annualmente i contenuti dell'Informativa completa rilasciata</p>	<p>E' stata presa visione dell'ultimo censimento dei trattamenti effettuati dall'Azienda, ne è stata verificata la coerenza con i contenuti dell'Informativa ed è stata aggiornata la data riportata sul documento.</p>	<p>√ Conforme ___ √ Non conforme ___ √ Parzialmente conforme ___ √ Non applicabile ___ Note:</p>
<p>Informativa Utenti sito web</p>	<p>Il ..... verifica annualmente i contenuti dell'Informativa completa rilasciata</p>	<p>E' stata presa visione dell'ultimo censimento dei trattamenti effettuati dall'Azienda, ne è stata verificata la coerenza con i contenuti dell'Informativa ed è stata aggiornata la data</p>	<p>√ Conforme ___ √ Non conforme ___ √ Parzialmente conforme ___ √ Non applicabile ___ Note:</p>

<sup>9</sup> Indicare il Soggetto che effettua la verifica: Responsabile del trattamento o Legale Rappresentante o Altri.

		riportata sul documento.	
Informativa Candidati all'Assunzione	Il ..... verifica annualmente i contenuti dell'Informativa completa rilasciata	E' stata presa visione dell'ultimo censimento dei trattamenti effettuati dall'Azienda, ne è stata verificata la coerenza con i contenuti dell'Informativa ed è stata aggiornata la data riportata sul documento.	<input checked="" type="checkbox"/> Conforme ___ <input checked="" type="checkbox"/> Non conforme ___ <input checked="" type="checkbox"/> Parzialmente conforme ___ <input type="checkbox"/> Non applicabile ___ Note:
Informativa Potenziali Clienti	Il ..... verifica annualmente i contenuti dell'Informativa completa rilasciata	E' stata presa visione dell'ultimo censimento dei trattamenti effettuati dall'Azienda, ne è stata verificata la coerenza con i contenuti dell'Informativa ed è stata aggiornata la data riportata sul documento.	<input checked="" type="checkbox"/> Conforme ___ <input checked="" type="checkbox"/> Non conforme ___ <input checked="" type="checkbox"/> Parzialmente conforme ___ <input type="checkbox"/> Non applicabile ___ Note:
Informativa Terzi (i.e.: Videosorveglianza)	Il ..... verifica annualmente i contenuti dell'Informativa completa rilasciata	E' stata presa visione dell'ultimo censimento dei trattamenti effettuati dall'Azienda, ne è stata verificata la coerenza con i contenuti dell'Informativa ed è stata aggiornata la data riportata sul documento.	<input checked="" type="checkbox"/> Conforme ___ <input checked="" type="checkbox"/> Non conforme ___ <input checked="" type="checkbox"/> Parzialmente conforme ___ <input type="checkbox"/> Non applicabile ___ Note:
.....	.....	.....	<input checked="" type="checkbox"/> Conforme ___ <input checked="" type="checkbox"/> Non conforme ___ <input checked="" type="checkbox"/> Parzialmente conforme ___ <input type="checkbox"/> Non applicabile ___ Note:

**PUNTO N°10**

**VERIFICA DELLE ATTIVITÀ DEGLI AMMINISTRATORI DI SISTEMA<sup>10</sup>**

*(Se tale misura necessaria di sicurezza non è applicata<sup>11</sup>, passare al Punto successivo)*

**Giudizio di conformità sugli adempimenti richiesti**

<b>Obiettivi di controllo</b>	<b>Presidio</b>	<b>Verifica effettuata</b>	<b>Grado di conformità</b>
<b>Censimento dei trattamenti</b>			
Tutti i trattamenti di dati personali effettuati anche con strumenti elettronici sono stati censiti e sono stati indicati i relativi AdS	Il ..... verifica annualmente i trattamenti di dati personali effettuati dalle Unità organizzative per aggiornare il censimento	E' stata presa visione dell'ultimo censimento dei trattamenti disponibile presso il Responsabile del trattamento e verificato che fosse completo	✓ Conforme ____ ✓ Non conforme ____ ✓ Parzialmente conforme ____ ✓ Non applicabile ____ Note:
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 AdS nell'ambito della propria organizzazione.	L'Informativa ai dipendenti prevede tale comunicazione	E' stata presa visione dell'Informativa ai dipendenti	✓ Conforme ____ ✓ Non conforme ____ ✓ Parzialmente conforme ____ ✓ Non applicabile ____ Note:

<sup>10</sup> L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, ad un'attività di verifica da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

<sup>11</sup> Dai destinatari del Provvedimento sono escluse le categorie dei Titolari dei trattamenti di dati personali effettuati con strumenti elettronici in ambito sia pubblico che privato a fini amministrativo-contabili che, ponendo minori rischi per gli Interessati, sono stati oggetto delle recenti misure di semplificazione ovvero:

- 1) amministrazioni pubbliche e società private che **utilizzano dati personali non sensibili** (nome, cognome, indirizzo, codice fiscale, numero di telefono) e che trattano come **unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori**, anche se extracomunitari, compresi quelli relativi al coniuge e ai parenti;
- 2) piccole e medie imprese, liberi professionisti o artigiani che **trattano dati solo per correnti finalità amministrativo-contabili**.

Ricordiamo che i trattamenti effettuati per finalità amministrativo-contabili sono quelli connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro.

<b>Lettera di Nomina AdS</b>			
Per ogni AdS è disponibile la Lettera di Nomina comprendente (al minimo)	Esiste uno modello di Lettera di Nomina ad AdS che prevede le caratteristiche richieste dalla legge		
√ Attestazione che l'Incaricato ha le caratteristiche richieste dalla legge;			√ Conforme ___ √ Non conforme ___ √ Parzialmente conforme ___ √ Non applicabile ___ Note:
√ Elencazione analitica degli ambiti di operatività richiesti e consentiti in base al profilo di autorizzazione assegnato			√ Conforme ___ √ Non conforme ___ √ Parzialmente conforme ___ √ Non applicabile ___ Note:
√ Indicazione delle verifiche almeno annuali che il Titolare svolgerà sulle attività svolte dall'AdS			√ Conforme ___ √ Non conforme ___ √ Parzialmente conforme ___ √ Non applicabile ___ Note:
√ Indicazione che la nomina ed il relativo nominativo sarà comunicato al personale ed eventualmente a terzi nei modi richiesti dalla legge			√ Conforme ___ √ Non conforme ___ √ Parzialmente conforme ___ √ Non applicabile ___ Note:

<b>Registrazione degli accessi</b>			
E' adottato un idoneo sistema per la registrazione degli access log (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli AdS	In Azienda è in uso il <i>software/hardware</i> ..... di gestione degli access log, tale sistema prevede il log degli accessi.	E' stata presa visione del <i>software/hardware</i> ..... e del manuale che ne descrive le caratteristiche.	<input checked="" type="checkbox"/> Conforme ___ <input checked="" type="checkbox"/> Non conforme ___ <input checked="" type="checkbox"/> Parzialmente conforme ___ <input checked="" type="checkbox"/> Non applicabile ___ Note:
Tali registrazioni (access log) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste	Il <i>software/hardware</i> ..... di gestione dei log conserva copia inalterabile dei log.	E' stata presa visione del <i>software/hardware</i> ..... e del manuale che ne descrive le caratteristiche	<input checked="" type="checkbox"/> Conforme ___ <input checked="" type="checkbox"/> Non conforme ___ <input checked="" type="checkbox"/> Parzialmente conforme ___ <input checked="" type="checkbox"/> Non applicabile ___ Note:
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	<input checked="" type="checkbox"/> Conforme ___ <input checked="" type="checkbox"/> Non conforme ___ <input checked="" type="checkbox"/> Parzialmente conforme ___ <input checked="" type="checkbox"/> Non applicabile ___ Note:
<b>Verifiche del Titolare</b>			
L'operato degli AdS è verificato, con cadenza almeno annuale, in modo da verificarne la sua rispondenza alle misure organizzative, tecniche, e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.	Annualmente viene verificato il rispetto degli obblighi normativi relativi agli AdS.	E' stata compilata la presente checklist	<input checked="" type="checkbox"/> Conforme ___ <input checked="" type="checkbox"/> Non conforme ___ <input checked="" type="checkbox"/> Parzialmente conforme ___ <input checked="" type="checkbox"/> Non applicabile ___ Note:

PUNTO N°11

PROGRAMMAZIONE DEGLI INTERVENTI FORMATIVI PRIVACY<sup>12</sup>

Formatore	Corso di Formazione	Descrizione sintetica	Numero di ore	Classi di Incarico Interessate	Calendario
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....

<sup>12</sup> L'obbligo formativo è previsto in termini sia di generale misura di sicurezza (art. 31) che di particolare misura minima di sicurezza (art. 33, 34 e 35).

**Il rischio del risarcimento danni cagionati a terzi**

Il Titolare di trattamento che non adempie all'obbligo formativo può inoltre vedersi costretto anche a rispondere per gli eventuali danni cagionati a terzi per effetto delle operazioni di trattamento per il semplice fatto di non aver adottato tutte le misure di sicurezza idonee a ridurre al minimo il rischio.

L'Art. 15 Codice Privacy dispone che: *“Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.”* che, tradotto, significa elevare l'attività di trattamento dati al rango di attività pericolosa.

Il Titolare che cagioni danno ad altri per effetto del trattamento di dati personali sarà *“...tenuto al risarcimento se non prova di aver adottato tutte le misure idonee a evitare il danno”*, tra le quali misure idonee, ovviamente, è inclusa la formazione privacy.

Per ottenere il risarcimento, l'Interessato dovrà soltanto dimostrare che:

- ✓ il danno si è realizzato
- ✓ il danno è dipeso dall'attività di trattamento posta in essere sotto il controllo del Titolare.

Il Titolare, quindi, per liberarsi della responsabilità, sarà costretto a dimostrare di avere adottato **tutte le misure possibili per impedire l'evento dannoso**, ovvero che che tra l'attività di trattamento e l'evento dannoso non vi è un nesso di causalità.

**La Formazione privacy come tutela del Titolare**

Se il danno deriva da negligenza o errore imputabile ad un Incaricato del trattamento, il Titolare potrà rivalersi su di essi se proverà di aver adottato tutte le cautele del caso, ed in particolare di aver **effettuato una corretta formazione privacy** mirata a rendere edotti gli Incaricati circa:

- ✓ i rischi che incombono sui dati,
- ✓ le misure disponibili per prevenire eventi dannosi,
- ✓ i profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività,
- ✓ le responsabilità che ne derivano
- ✓ le modalità per aggiornarsi sulle misure minime adottate dal titolare.

In conclusione: il Titolare che abbia effettuato una corretta formazione privacy, oltre ad applicare le sanzioni disciplinari previste (art. 2106 c.c.) potrà rivalersi sui lavoratori per inadempimento contrattuale richiedendo il risarcimento dei danni subiti.

**PUNTO N°12**  
**DICHIARAZIONI D'IMPEGNO E FIRMA**

Il presente documento, redatto in data ....., viene siglato in ogni sua pagina e firmato in calce da:

➤ ..... in qualità di .....

L'originale del presente documento viene custodito presso il .....<sup>13</sup> della scrivente Organizzazione, per essere esibito in caso di controlli.

Luogo e data .....

Firma

.....

---

<sup>13</sup> Indicare il Responsabile Privacy