

CHECK LIST ADEGUAMENTO NUOVO REGOLAMENTO PRIVACY

DENOMINAZIONE AZIENDA <hr/>
CODICE FISCALE _____ P. IVA _____
ANNOTAZIONI <hr/>

Nome del Titolare del Trattamento	Indirizzo: Numero di tel: Indirizzo e-mail Indirizzo PEC
Nome del Responsabile per la protezione dei dati personali (DPO)	Indirizzo: Numero di tel: Indirizzo e-mail: Indirizzo PEC:

CHECK LIST		
ADEGUAMENTO NUOVO REGOLAMENTO PRIVACY	SI	NO
<b style="color: red;">1. E' stata scritta una <i>informativa</i> sulla protezione dei dati? E' messa a disposizione dei vostri clienti, partners e dipendenti?	<input type="checkbox"/>	<input type="checkbox"/>
<p>Il GDPR prevede la creazione di una informativa sulla protezione dei dati per documentare il loro trattamento. Tale documentazione dovrà essere scritta in una forma semplice e chiara, descrivere il fine della raccolta dati, i diritti del proprietario dei dati, se tali dati saranno trasferiti all'estero e con quali strumenti, il periodo di conservazione, ecc... [artt. 13 e 14].</p> <p>L'informativa migliorerà la comprensibilità delle logiche di trattamento dei dati personali da parte delle autorità di vigilanza e da parte dei clienti, rafforzando quindi la loro fiducia.</p>		

<p>2. Avete strutturato la protezione dei dati secondo il concetto <i>Data Protection by Design</i>?</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali — nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento [art. 24].</p> <p>E' dunque necessario configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati [art. 25].</p>		
<p>3. Avete redatto una analisi dei rischi relativa al trattamento dei dati?</p>		
<p>Tra gli obblighi fondamentali del titolare del trattamento vi è quello di individuare e mitigare i rischi inerenti il trattamento [Considerando 75, 76, 77 – pag. 46 e 47].</p> <p>Questi ultimi sono da intendersi come il rischio di impatti negativi sulle libertà ed i diritti degli interessati. Tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione [artt. 35 e 36] tenendo conto dei rischi noti e delle misure tecniche e organizzative che il titolare ritiene di dover adottare per mitigare tali rischi.</p> <p>Il titolare potrà decidere in autonomia, in base all'esito della valutazione, se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) oppure consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuo.</p> <p>L'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento [art. 36, par. 2].</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>4. Avete nominato un Responsabile della Protezione dei Dati?</p>	<input type="checkbox"/>	<input type="checkbox"/>

<p>La nomina di un Responsabile della Protezione dei Dati (acronimo inglese "DPO") è obbligatoria quando il trattamento e le attività principali</p> <ul style="list-style-type: none"> • sono svolte da un organismo pubblico • consistono in elaborazioni che richiedono un controllo regolare e sistematico dei dati • consistono in elaborazioni su larga scala di dati sensibili o di rilevanza penale <p>Poiché il Garante incoraggia la designazione del DPO, in via cautelativa può essere utile nominarlo su base volontaria, resta inteso che l'azienda dovrà assicurare al Responsabile tutti i mezzi necessari per lo svolgimento del suo ruolo [artt. 37 e 38].</p>		
<p>5. Avete un registro dei trattamenti?</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Il Regolamento ha rimosso gli obblighi di notifica dei trattamenti, costosi e inefficienti, previsti dalla direttiva tuttora vigente, sostituendo tale prescrizione con la tenuta di un <i>registro dei trattamenti</i>, che è esteso anche ai fornitori esterni che trattano dati personali. Tale registro deve essere presentato in forma scritta, anche elettronica, e tenuto a disposizione dell'autorità di vigilanza [art. 30].</p> <p>Le aziende con meno di 250 dipendenti sono esentate da quest'obbligo a meno che:</p> <ul style="list-style-type: none"> · L'elaborazione comporti un rischio elevato per i diritti e le libertà degli individui · L'elaborazione non è occasionale · L'elaborazione riguardi dati sensibili 		
<p>6. Avete offerto ai vostri dipendenti formazione o campagne di sensibilizzazione in tema di protezione dei dati personali?</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Uno dei compiti del Responsabile della Protezione dei Dati è quello di aumentare la sensibilizzazione e fornire la formazione a tutti i dipendenti dell'azienda e, in particolare, al personale coinvolto nel trattamento dei dati personali [art. 39].</p>		
<p>7. Durante la raccolta dei dati personali dei vostri clienti e dipendenti viene usato un processo di consenso esplicito e specifico?</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Nessun consenso è valido in caso di silenzio assenso, di casella selezionata di default o di inattività della persona [artt. 9 e 22]. Inoltre il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali [art. 7].</p>		

8. Siete in grado di dare alle persone l'accesso a tutti i loro dati personali?	<input type="checkbox"/>	<input type="checkbox"/>
Occorre adottare misure per fornire agli individui i mezzi per richiedere ed accedere ai propri dati personali a titolo gratuito, in modo che essi possano liberamente modificare, cancellare o esercitare la loro opposizione al trattamento [art. 15].		
9. Siete in grado di aggiornare o cancellare i dati personali dei vostri clienti?	<input type="checkbox"/>	<input type="checkbox"/>
Il diritto di rettifica prevede che una persona possa ottenere, nel più breve tempo possibile, la cancellazione o la rettifica dei propri dati personali inesatti o incompleti [art. 15]. In alternativa alla cancellazione è previsto che l'interessato possa anche chiedere la limitazione al trattamento dei suoi dati [art. 18].		
10. Esiste una procedura per la conservazione dei dati personali?	<input type="checkbox"/>	<input type="checkbox"/>
La conservazione dei dati trattati in violazione dei diritti degli interessati rappresenta un trattamento illecito passibile di sanzioni amministrative. Il periodo di conservazione non deve superare il tempo necessario per l'effettuazione degli scopi per i quali i dati sono stati raccolti [art. 15].		
11. Siete in grado di soddisfare il diritto dei vostri clienti in merito alla portabilità dei loro dati?	<input type="checkbox"/>	<input type="checkbox"/>
Una persona ha il diritto di ricevere i propri dati personali in un formato strutturato, comunemente usato e leggibile da un computer. La persona può anche richiedere al titolare l'invio in forma elettronica dei dati che lo riguardano [art. 20].		
12. Esiste un sistema per gestire l'accesso sicuro agli archivi contenenti dati personali?	<input type="checkbox"/>	<input type="checkbox"/>
I dati personali devono essere trattati in modo tale da garantire la sicurezza e la riservatezza, anche per mezzo di sistemi di autenticazione ed autorizzazione [art. 32].		
13. Nel caso di un incidente di sicurezza che coinvolga dati personali, è stato creato un processo di gestione dell'incidente e della sua notifica?	<input type="checkbox"/>	<input type="checkbox"/>
Nel caso di un'emergenza o di un incidente che coinvolge dati personali, il Responsabile della Protezione dei Dati deve garantire un processo di gestione dell'incidente e relativa notifica al Garante. Innanzitutto l'incidente deve essere documentato, evidenziando le circostanze, le conseguenze e le misure adottate. Per scongiurare la notifica agli interessati occorre riuscire a dimostrare al Garante di avere posto in essere tutte le misure di sicurezza ragionevolmente adottabili per impedire l'incidente [artt. 33 e 34].	<input type="checkbox"/>	<input type="checkbox"/>
14. Quali misure adottate per quanto riguarda i vostri fornitori? Il contratto che disciplina la fornitura garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza?	<input type="checkbox"/>	<input type="checkbox"/>

<p>Al fine di rispettare la Normativa, un subappaltatore o fornitore che agisce per conto di una azienda deve rispettare le garanzie necessarie in termini di conoscenze specializzate, affidabilità e sicurezza del trattamento.</p> <p>L'elaborazione da parte di un fornitore deve essere disciplinata da un atto giuridico vincolante per entrambe le parti, che definisce la finalità e la durata del trattamento, il tipo di dati personali e le categorie di persone coinvolte [art. 28].</p>		
<p>15. Esiste una procedura per il trasferimento di dati al di fuori dell'Unione Europea?</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>In caso di trasferimenti di dati personali verso un Paese terzo, deve essere mantenuto un registro delle attività di trasferimento, tra cui l'identificazione del Paese terzo e dei documenti provanti l'esistenza di adeguate garanzie per il trasferimento [art. 47, par. 2 comma B].</p> <p>Il regolamento vieta trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di decisioni giudiziarie o di ordinanze amministrative emesse da autorità di tale Paese terzo, a meno dell'esistenza di accordi internazionali, in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati [art. 48].</p>		