



Autodichiarazione

ALLEGATO B.4
AL
DISCIPLINARE

Responsabile (esterno) del trattamento

Pag. 1 di 6

RAGIONE SOCIALE/NOME DEL RESPONSABILE DEL TRATTAMENTO	
NOME E RECAPITI (TEL, EMAIL) DEL COMPILATORE DELLA PRESENTE	

SEZIONE A – DATI PERSONALI E MODALITÀ DEL TRATTAMENTO

Requisito		Risposta
1	Vengono trattate tipologie di dati personali diverse da quelle indicate nell'Atto di Nomina a Responsabile del Trattamento?	
2	Vengono trattati dati personali di interessati diversi da quelli elencati nell'Atto di Nomina a Responsabile del Trattamento?	
3	I dati personali vengono e/o verranno trattati per finalità diverse da quelle indicate nell'Atto di Nomina a Responsabile del Trattamento?	
4	Dove avviene il trattamento dei dati personali da parte del Responsabile, del suo Personale Autorizzato e di eventuali ulteriori Sub-responsabili?	

SEZIONE B - MISURE ORGANIZZATIVE

Requisito		Risposta
1	Tutto il Personale Autorizzato è stato appositamente nominato tale per il trattamento ricevendo le istruzioni di cui al presente Atto di Nomina?	
2	Il Personale Autorizzato effettua dei corsi di formazione annuale in merito agli obblighi previsti dal GDPR e dalle altre normative in materia di protezione dei dati personali?	
3	Esiste un registro delle attività di trattamento dei dati personali? In caso di risposta positiva, viene regolarmente aggiornato?	
4	È stato nominato un Responsabile della Protezione dei Dati (DPO in inglese)? <i>(specificare se l'Ente non è obbligato a</i>	

**Autodichiarazione****Responsabile (esterno) del trattamento**

Requisito		Risposta
	<i>nominare il DPO)</i>	
5	Vengono adottate delle misure organizzative interne volte ad evitare trattamenti dei dati personali in violazione degli obblighi di cui all'Atto e violazioni di dati personali?	
6	Esiste un indirizzo email o call center dedicato per la notifica delle violazioni di dati personali?	
7	Prima di procedere alla nomina di eventuali ulteriori Sub-Responsabili, è stata richiesta l'autorizzazione scritta al Titolare?	
8	È stata verificata (ed è verificata almeno con cadenza annuale) l'adeguatezza delle misure tecniche e organizzative di ogni eventuale ulteriore Sub-Responsabile tramite la compilazione della presente Checklist di Conformità al momento dell'attribuzione dell'incarico, e con cadenza annuale?	
9	Gli eventuali ulteriori Sub-Responsabili del trattamento sono stati nominati tali sulla base di un accordo i cui contenuti sono sostanzialmente analoghi al presente Atto?	
10	Sono individuate le modalità di conferimento dell'informativa all'interessato e sono individuati gli autorizzati tenuti a verificare che l'informativa sia stata oggetto di presa visione ovvero, ove necessario, che vi sia stata manifestazione del consenso	

SEZIONE C - MISURE TECNICHE

Requisito		Risposta
1	Esistono misure tecniche in grado di tracciare il trattamento dei dati personali nei sistemi informatici?	
1.1	Se trattate le particolari categorie di dati personali è previsto un accesso / autorizzazione separata e/o specifica per il soggetto autorizzato, distinta rispetto a quella che autorizza il trattamento degli altri dati personali? Se sì, quale?	
2	Esistono misure tecniche in grado di tracciare i dati personali in formato cartaceo?	

**Autodichiarazione****Responsabile (esterno) del trattamento**

Requisito		Risposta
2.1	Se trattate le particolari categorie di dati personali è previsto un accesso / autorizzazione separata e/o specifica per il soggetto autorizzato, distinta rispetto a quella che autorizza il trattamento degli altri dati personali? Se sì, quale?	
3	Esistono delle misure tecniche volte ad identificare e/o prevenire eventuali trattamenti dei dati personali secondo finalità diverse da quelle previste dall'Atto?	
4	Esistono delle misure tecniche in grado di consentire la cancellazione, la modifica, l'aggiornamento, la limitazione del trattamento e la portabilità dei dati personali a richiesta del Titolare e/o alla cessazione dell'Atto?	
5	Esistono delle misure tecniche che consentono la restituzione dei dati personali al Titolare, a richiesta della stessa e/o alla cessazione dell'Atto?	<i>[in caso di risposta positiva, descrivere le misure adottate]</i>
6	Gli accessi degli incaricati ai sistemi informatici sono protetti tramite <i>codice-id</i> e <i>password</i> ?	
7	La <i>password</i> di accesso ai sistemi informatici utilizzata da ogni Persona Autorizzata è di almeno 8 caratteri, non facilmente riconducibile all'incaricato (quindi non uguale alla <i>log-in</i>) e modificata al primo utilizzo e ogni 3 mesi?	
8	Vengono utilizzati account condivisi tra più Persone Autorizzate per poter accedere ai dati personali?	
9	Il <i>codice-id</i> delle Persone Autorizzate è personale e non viene assegnato a più soggetti, neppure in tempi diversi?	
10	Le credenziali di autenticazione non utilizzate da almeno 6 mesi vengono disattivate?	
11	Esistono delle misure tecniche che consentono l'accesso ai dati personali unicamente al Personale Autorizzato che deve accedervi per eseguire le attività previste dall'Atto?	

**Autodichiarazione****Responsabile (esterno) del trattamento**

Requisito		Risposta
12	Vengono revisionati i profili di accesso ai sistemi informatici con cadenza almeno annuale per accertare la loro correttezza?	
13	I permessi di accesso vengono disabilitati quando il Personale Autorizzato non ha più diritto di accedere ai dati personali?	
14	Sono state adottate misure volte a minimizzare gli effetti negativi per gli interessati in caso di violazione dei dati personali (es. pseudonimizzazione o criptazione)?	
15	Esiste una procedura di emergenza e di <i>business continuity</i> da seguire in caso di violazione di dati personali?	
16	Vengono eseguite copie di <i>backup</i> dei dati personali?	
17	Vengono aggiornati i sistemi antivirus e firewall?	
18	Vengono eseguiti <i>penetration test</i> e <i>vulnerability assessment</i> (VAPT) dei sistemi informatici che trattano i dati personali?	
19	Esistono altre procedure tecniche periodiche che vengono eseguite per verificare l'adeguatezza delle misure di sicurezza volte a proteggere l'accesso ai dati personali?	
19	I documenti cartacei contenenti i dati personali sono custoditi in armadi con chiusura a chiave?	
20	L'accesso ai locali in cui sono custoditi i dati personali è controllato tramite badge di riconoscimento o altre forme di controllo?	
21	Esiste una politica aziendale che disciplina la distruzione dei documenti dopo lo scadere del termine di legittima conservazione dei dati personali?	
22	Esistono strumenti atti a distruggere i documenti cartacei in modo irreversibile? (es. tritacarte elettrici)	
23	Esistono strumenti atti a distruggere i documenti informatici in modo irreversibile? (es. programmi di vaporizzazione)	
24	Sono utilizzati telefoni o tablet aziendali o pc portatili aziendali?	



Autodichiarazione

Responsabile (esterno) del trattamento

ALLEGATO B.4
AL
DISCIPLINARE

Pag. 5 di 6

Requisito		Risposta
25	In caso di risposta affermativa alla domanda precedente è stata adottata una politica aziendale relativa alle modalità di utilizzo dei device aziendali (password, conservazione dei device, utilizzo dei device solo per finalità lavorative, etc.)	
26	Sono utilizzati per l'esercizio delle attività device personali (telefoni, tablet, pc)	
27	In caso di risposte affermative alle domande 24 - 26, è previsto che l'archiviazione dei files di rilevanza aziendale si abbia solo su cloud o gestionale aziendale	

SEZIONE D - STORICITA'

Requisito		Risposta
1	Vi sono mai stati casi di sottrazione, distruzione, perdita di dati personali (furti pc, accesso abusivo al sistema informatico aziendale, etc.)	
1.1	In caso di risposta affermativa alla domanda precedente descrivere sommariamente le conseguenze (conseguenze gravi, di media gravità, tenui, considerando il danno alla persona fisica, le sanzioni irrogate, le azioni giudiziarie conseguenti)	
2	Vi sono state richieste di cancellazione dei dati personali (diritto all'oblio)?	
2.1	In caso di risposta affermativa indicare se le stesse sono frequenti, rare o rarissime	
3	Vi è mai stato un contenzioso in materia di dati personali in caso di risposta affermativa: <ul style="list-style-type: none">• dinanzi al Garante per la protezione dei dati personali• dinanzi al Tribunale Civile• dinanzi al Tribunale Penale	
4	In caso di risposta affermativa alla precedente domanda v'è stata una condanna dell'Ente o di un suo collaboratore / amministratore	



Autodichiarazione
Responsabile (esterno) del trattamento

Data

Timbro e firma Responsabile (esterno) del Trattamento*

*** NB. La firma del titolare, del legale rappresentante o persona da questi appositamente delegata.**