CHECKLIST DI VERIFICA DEL RESPONSABILE
per l'adeguamento al Regolamento Generale sulla Protezione dei Dati Personali 2016/679 (GDPR)

Nell'ottica di garantire un corretto trattamento dei dati personali e consentirne una lecita circolazione, il Regolamento Europeo 2016/679 (GDPR) richiede di porre in essere misure tecniche e organizzative in grado di soddisfare adeguati requisiti di sicurezza.

Qualora un trattamento debba essere effettuato per conto del Titolare ad opera di terzi Responsabili, il Regolamento richiede l'adozione ad opera di questi ultimi di idonee misure tecnico-organizzative.

Vi invitiamo a compilare la seguente check list al fine di valutare che le garanzie che la Vostra organizzazione presenta siano adeguate alla soddisfazione dei requisiti richiesti dal GDPR, nonché alla tutela dei diritti degli interessati coinvolti nel trattamento che effettua per conto del Titolare.

Responsabile del Trattamento	
Checklist completata da	
Data	

Sezione A – Dati e modalità del Trattamento

	Domande	Risposte	Competenza Valutazione Risposta
1	Trattate per conto del Titolare dati personali, oltre quelli indicati nella nomina ex art. 28 e/o contratto?		AA.GG.
2	Trattate per conto del Titolare dati personali di altre categorie di interessati, oltre quelle indicate nella nomina ex art. 28 e/o contratto?		AA.GG.
3	I Dati Personali sono e/o saranno trattati - per conto del Titolare - per finalità / scopi diversi da quelli indicati nella nomina ex art. 28 e/o contratto?		AA.GG.
4	Specificare i luoghi (indicando anche dove si trovano i server, se presenti) dove il Responsabile, gli autorizzati al trattamento e gli eventuali Sub-responsabili trattano i dati personali per conto del Titolare.		AA.GG. / Sistemi Informatici
5	Precisare se l'hosting e gli ulteriori trattamenti dei dati personali effettuati per conto del Titolare, sono limitati allo Spazio economico europeo (SEE).		Sistemi Informatici
6	Nel caso in cui i dati personali siano trattati per conto del Titolare al di fuori del SEE, descrivere le misure di salvaguardia ai sensi degli artt. 46 e 47 GDPR per garantire che siano adeguatamente protetti al di fuori del SEE (per esempio: Clausole Contrattuali Standard Europee).		AA.GG.

Sezione B – Misure organizzative

Domande	Risposte	Competenza Valutazione Risposta

1	E' stato delineato un sistema interno di deleghe di compiti e funzioni in materia di privacy?	[*In questo caso, si prega di descrivere la/le misura/e adottate*]	AA.GG.
2	Il personale è stato autorizzato al trattamento secondo profilazioni definite?		AA.GG.
3	Tutti gli autorizzati al trattamento hanno ricevuto le istruzioni per il trattamento dei dati personali nel quale sono coinvolti mediante lettera di incarico (art 29 GDPR)?		
4	Tutte le persone autorizzate al trattamento partecipano, su base annuale, a corsi di formazione incentrati sugli obblighi previsti dalle normative vigenti in tema di Protezione dei Dati?		AA.GG.
5	Avete adottato un registro delle attività di Trattamento[1] (art 30 GDPR) in qualità di Responsabile? Se così fosse, questo registro è sempre aggiornato?		AA.GG.
6	E' stato compilato il documento di valutazione dei rischi?		AA.GG.
7	Viene eseguita la valutazione di impatto privacy[2]?		AA.GG.
8	E' obbligatoria la valutazione d'impatto privacy[2]?		AA.GG.
9	È stato nominato il Data Protection Officer?		AA.GG.
10	Avete adottato misure organizzative interne volte a prevenire / gestire eventuali violazioni in merito al trattamento di dati personali da parte degli autorizzati al trattamento dei dati personali (procedura di data breach ai sensi degli artt. 33 e 34 GDPR)?		AA.GG. / Sistemi Informatici
11	Avete un indirizzo e-mail o call center dedicato dove possono essere segnalate violazioni dei dati personali (procedura di data breach ai sensi degli artt. 33 e 34 GDPR)?		AA.GG. / Sistemi Informatici
12	Avete dei Sub-Responsabili per la fornitura dei servizi offerti al Titolare del trattamento? In caso affermativo, avete richiesto l'autorizzazione scritta al Titolare del trattamento prima di ricorrere ad eventuali Sub-Responsabili per l'esecuzione di specifiche attività di trattamento? Si prega produrre elenco dei Sub-Responsabili aggiornato alla data di compilazione della presente Checklist.		AA.GG.
13	Ogni Sub-Responsabile è tenuto a compilare questa Checklist sia al momento della sua nomina, sia con cadenza annuale. Avete verificato (e verificate almeno una volta all'anno) l'adeguatezza delle misure tecniche e organizzative di ciascun Sub-Responsabile autorizzato, attraverso la presente Checklist?		AA.GG.
14	Ciascun Sub-Responsabile viene nominato sulla base di un atto il cui contenuto è sostanzialmente conforme a quello intercorrente tra il Titolare ed il Responsabile relativamente a doveri e responsabilità del Sub-Responsabile?		AA.GG.

[1]Art. 30,c. 5, Reg. UE n. 679/2016: "Gli obblighi (di tenuta del registro) non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'art. 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'art. 10".

[2] Art. 32, c. 1, Reg. UE n. 679/2016: "….il titolare del trattamento e il Responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio".

Sezione C – *Misure tecniche*

	Domande	Risposte	Competenza Valutazione Risposta
1	Disponete di misure tecniche per garantire un adeguato livello di sicurezza all'interno dei sistemi IT utilizzati nel trattamento di dati effettuato per conto del Titolare?	[*In questo caso, si prega di descrivere la/le misura/e adottate*]	Sistemi Informatici
2	Avete predisposto misure tecniche volte a prevenire il trattamento di dati personali per scopi diversi da quelli previsti dall'Addendum? (es. I dati personali non devono poter essere copiati su supporti rimovibili, ad eccezione dei supporti espressamente autorizzati dal Responsabile per attività specifiche)	[*In questo caso, si prega di descrivere la/le misura/e adottate*]	Sistemi Informatici
3	Disponete di misure tecniche in grado di consentire la cancellazione, la rettifica, l'aggiornamento, la limitazione del trattamento e la portabilità dei Dati personali su richiesta del Titolare e/o al termine del contratto intercorrente con lo stesso?	[*In questo caso, si prega di descrivere la/le misura/e adottate*]	Sistemi Informatici
4	Disponete di misure tecniche in grado di consentire la restituzione dei dati personali al Titolare, su sua richiesta e/o al termine del contratto?	[*In questo caso, si prega di descrivere la/le misura/e adottate*]	Sistemi Informatici
5	Gli accessi delle persone autorizzate al trattamento ai sistemi IT sono protetti da ID e password personali?		Sistemi Informatici
6	La password che ogni autorizzato al trattamento utilizza per accedere ai sistemi IT, è formata da almeno 8 caratteri, non facilmente riferibile all'autorizzato (cioè diversa dalla sua password di accesso) e modificata quando usata per la prima volta e ogni 3 mesi?		Sistemi Informatici
7	Le persone autorizzate al trattamento utilizzano account condivisi per accedere ai dati personali?	[*In questo caso, si prega di descrivere per quali ragioni esistano tali account condivisi e quanti sono*]	Sistemi Informatici
9	Disattivate le credenziali di autenticazione che non vengono utilizzate da almeno 6 mesi?		Sistemi Informatici
10	Disponete di misure tecniche che consentono l'accesso ai dati personali solo a Sub-Responsabili del Trattamento autorizzati da apposita nomina/contratto di servizi?		AA.GG. / Sistemi Informatici
11	I profili di accesso ai sistemi IT vengono riesaminati almeno una volta all'anno per verificare che siano corretti, secondo un principio di profilazione degli accessi che tenga conto del ruolo e delle responsabilità di ciascun utente/autorizzato al trattamento?		Sistemi Informatici
12	Le credenziali di accesso sono disattivate quando l'autorizzato al trattamento non ha più diritto di accedere ai dati personali (ad esempio, per cessazione del rapporto di lavoro o cambio di mansione)?		Sistemi Informatici

13	Gli accessi amministrativi individuali da remoto ai sistemi che gestiscono i dati personali sono protetti mediante un meccanismo di autenticazione che richiede modifica della password ogni 90 giorni? Si consiglia di dotarsi di strumenti per la gestione delle password (tool ad hoc) per garantire la sicurezza delle credenziali.		Sistemi Informatici
14	L'accesso da remoto (da reti esterne) agli ambienti che trattano dati personali è protetto mediante autenticazione a più fattori?		Sistemi Informatici
15	Avete adottato misure volte a ridurre al minimo il rischio che gli interessati siano identificati e misure volte a mitigare gli effetti negativi per gli interessati in caso di violazione dei dati personali? (es. pseudonimizzazione, crittografia, visibilità dei dati personali limitata al solo set di informazioni necessario per le singole attività di elaborazione).	[*In questo caso, si prega di indicare tali misure*]	Sistemi Informatici
16	Avete in atto una procedura di emergenza e di business continuity da seguire in caso di violazione dei dati personali?	[*In questo caso, si prega di descrivere tale procedura o allegarla alla presente checklist*]	Sistemi Informatici
17	Il backup dei dati personali è eseguito almeno una volta alla settimana?		Sistemi Informatici
18	I sistemi antivirus e firewall sono aggiornati almeno una volta al mese?		Sistemi Informatici
19	I sistemi IT, mediante i quali vengono trattati i dati personali, sono sottoposti, almeno una volta all'anno, a penetration test o vulnerability assessment?		Sistemi Informatici
20	Avete in essere altre procedure tecniche che vengono regolarmente eseguite al fine di verificare l'adeguatezza delle misure di sicurezza volte a proteggere l'accesso ai dati personali?	[*In questo caso, si prega di descrivere tale procedura o allegarla alla presente checklist*]	Sistemi Informatici
21	Adottate sistemi di avviso in caso di trasferimento di grandi quantità di dati personali, violazioni dei dati personali o attacchi informatici (come DDoS - Distributed Denial of Service)?		Sistemi Informatici
22	Tutti i supporti cartacei contenenti i dati personali sono conservate in armadi chiusi?		AA.GG.
23	L'accesso ai luoghi in cui vengono conservati i dati personali viene controllato tramite un sistema di badge o qualsiasi altra forma di controllo?		AA.GG.
24	I documenti cartacei e i supporti magnetici/ottici (ad es. dischi rigidi, DVD, CD, smart card, chiavette USB) vengono distrutti o resi inutilizzabili per garantire che i dati e le informazioni in essi contenuti non possano essere ricostruiti e/o utilizzati (anche parzialmente) da terze parti non autorizzate? I documenti cartacei vengono fisicamente distrutti prima di essere cestinati attraverso dispositivi specifici quali distruggi documenti?		Sistemi Informatici

25	Avete adottato misure volte a prevenire la lettura, la copia, la modifica o la cancellazione non autorizzate di dati personali durante il loro eventuale trasferimento o durante il trasporto di supporti contenenti i dati?	[*In questo caso, si prega di descrivere tali misure*]	Sistemi Informatici
26	L'archiviazione di database/archivi di dati è basata su una classificazione appropriata degli asset, in base al livello di criticità? Ad esempio, i database/data storage che vengono utilizzati per la memorizzazione di una grande quantità di dati personali sono protetti tramite strong encryption? In caso affermativo, quale granularità è applicata?		Sistemi Informatici
27	Per la dismissione degli asset IT sono messe in atto procedure di pulizia sicura al fine di rimuovere tutti i dati personali e/o sovrascrivere in modo sicuro prima dello smaltimento o del riutilizzo dello strumento?		Sistemi Informatici
28	Firewall e router sono configurati al fine di limitare il traffico, in entrata e in uscita, da reti "non attendibili" (inclusi wireless) ed i sistemi? E' negato tutto il resto del traffico ad eccezione dei protocolli necessari all'ambiente che tratta dati personali?		Sistemi Informatici
29	I firewall delle applicazioni sono configurati davanti ai server Web appartenenti all'ambiente che tratta dati personali, al fine di verificare e convalidare il traffico che è diretto al server? Qualsiasi servizio o traffico non autorizzato viene bloccato e viene generato un avviso?		Sistemi Informatici
30	I dati di produzione sono consentiti e limitati solo agli ambienti di produzione. In casi eccezionali e con le approvazioni necessarie, gli ambienti di test e di sviluppo possono elaborare dati personali (reali) nella misura in cui siano protetti come gli ambienti di produzione. Gli ambienti di test e di sviluppo, così come quelli di pre-produzione utilizzano dati resi anonimi?		Sistemi Informatici
31	Proteggete i dati personali durante la trasmissione su reti aperte, pubbliche o non attendibili, con l'implementazione della strong cryptography o l'utilizzazione di protocolli sicuri?		Sistemi Informatici
32	Sono utilizzati strumenti di sicurezza per monitorare e controllare il flusso di dati personali attraverso gli endpoint e verso le reti esterne?		Sistemi Informatici
33	L'accesso agli ambienti di produzione contenenti dati personali e in generale l'accesso ai sistemi contenenti dati personali del Titolare del trattamento sono monitorati e loggati al fine di tracciare l'accesso dell'utente Amministratore di Sistema che accede ai dati personali? Si precisa che, in caso di necessità e/o di prescrizione normativa, il Titolare del trattamento dei dati personali ha il diritto di ottenere i log dai Responsabili del trattamento e/o dai Sub-responsabili.		Sistemi Informatici

34	Le registrazioni (access log) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al rispetto della normativa?		Sistemi Informatici
35	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?		Sistemi Informatici
36	Sono stati comunicati al Titolare del trattamento i nominativi degli AdS nominati dal Responsabile?		AA.GG. / Sistemi Informatici
37	PRIVACY BY DESIGN: In caso di fornitura di software e/o APP, viene garantita la conformità privacy by design prevista dal GDPR? Indicare la conformità		Sistemi Informatici

Firma del Legale Rappresentante del Responsabile:

Data: _____.../.../2019_____

Nome: _____

Firma: _____