Allegato 2

Questionario di Conformità del Fornitore al GDPR

L'art. 28 del GDPR prevede che il Titolare possa ricorrere unicamente a Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato. Questo **Questionario di Conformità al GDPR** mira a valutare la conformità del Fornitore al GDPR 2016/679.

A tal fine chiediamo al fornitore di rispondere alle seguenti domande

Ragione sociale dell'Azienda Fornitrice	
Compilatore (indicare il nome di chi compila il documento)	
Data di compilazione	
Breve descrizione dell' attività svolta per conto del Titolare del Trattamento	

1) **Il trattamento dei dati svolto per conto del Titolare è stato strutturato nel rispetto della Data protection by design e nel rispetto delle - "Misure minime di sicurezza ICT per le pubbliche amministrazioni" stabilite da AGID con la circolare del 18 aprile 2017, n. 2/2017 pubblicata sulla Gazzetta Ufficiale. L'elenco delle misure è descritto all'indirizzo: https://www.agid.gov.it/it/sicurezza/misure-minime- sicurezza-ict.**

   - ☐ SI
   - ☐ NO

2) **Sussistono certificazioni rispetto al servizio erogato al Titolare?**

   - ☐ ISO 27001
   - ☐ ISO 9001
   - ☐ SAAS
   - ☐ ALTRE_____
   - ☐ NO

3) **Sussistono polizze assicurative rispetto al servizio erogato al Titolare?**

   - ☐ SI (specificare) _____
   - ☐ NO

4) **E' stata condotta la DPIA (analisi dei rischi) relativa al trattamento dei dati oggetto del trattamento?**

   - ☐ SI
   - ☐ NO

5) **Se è stata condotta la DPIA (analisi dei rischi) quale metodologia viene usata per calcolare il rischio?**

- ☐ ISO 27001
- ☐ ENISA
- ☐ Altro specificare:_____

6) **Il risultato del calcolo del rischio residuale della DPIA (analisi dei rischi) sul trattamento dei dati del Titolare è risultato**

- ☐ BASSO
- ☐ MEDIO
- ☐ ALTO
- ☐ MOLTO ALTO

7) **E' stata condotta la valutazione d'impatto sul trattamento dei dati personali del Titolare?**

- ☐ SI ALLEGARE COPIA DELLA VALUTAZIONE
- ☐ NON E' NECESSARIO (specificare):_____
- ☐ NO

8) **Nel caso di trattamenti di dati personali di minori sono state previste misure aggiuntive?**

- ☐ SI
- ☐ NO

9) **Avete designato il Responsabile della protezione dei dati personali?**

- ☐ SI (specificare) _____
- ☐ NON E' OBBLIGATORIO/NON E' STATO CONSIDERATO OBBLIGATORIO
- ☐ NO

10) **Avete redatto il Registro dei trattamenti in qualità di Responsabile del trattamento per i trattamenti effettuati per conto del Titolare?**

- ☐ SI
- ☐ NO
- ☐ NON E' OBBLIGATORIO/NON E' STATO CONSIDERATO OBBLIGATORIO

Altro specificare:
_____
_____

11) **Per ogni trattamento svolto per conto del Titolare siete in grado, su richiesta, di fornire:**

- ☐ LOCALIZZAZIONE
- ☐ ASSET
- ☐ ELENCO DEI SOGGETTI AUTORIZZATI
- ☐ SUB-RESPONSABILI

 TEMPO DI CONSERVAZIONE DEI DATI

12) E' presente un organigramma GDPR nel quale sono evidenziate tutte le persone che trattano i dati personali del Titolare?

 SI
 NO

13) Il personale che ha accesso ai dati del Titolare è stato designato, ha ricevuto istruzioni specifiche ed è vincolato alla riservatezza?

 SI
 NO

14) Il personale che ha accesso ai dati del Titolare è stato formato in tema di trattamento di dati personali?

 SI
 NO

15) Avete previsto profili di autorizzazione personalizzati per ogni autorizzato che ha accesso ai dati o ai sistemi del Titolare e una policy che gestisce la comunicazione tempestiva in caso di arrivo/cambio di mansione/dimissione e la relativa comunicazione anche al Titolare quando hanno accessi diretto ai sistemi del Titolare?

 SI (specificare): _____
 NO

16) Periodicamente, con cadenza almeno annuale, sono aggiornati gli ambiti di trattamento consentito agli autorizzati e ai responsabili della gestione e manutenzione dei sistemi elettronici?

 SI (specificare): _____
 NO
 NON E' NECESSARIO (specificare):_____

17) Con riferimento al Provvedimento emanato dall'Autorità Garante per la protezione dei dati personali, in materia di amministratori di sistema (novembre 2008) indicare quanto segue:

- Ogni amministratore accede con credenziali nominative?

 SI
 NO
 NON E' NECESSARIO (specificare):_____

- Sono presenti le nomine ad amministratori di sistema?

 SI
 NO
 NON E' NECESSARIO (specificare):_____

- Sono presenti amministratori esterni?

□ SI
□ NO
□ NON E' NECESSARIO (specificare):_____

- E' redatta annualmente la relazione in materia di amministratore di sistema?

□ SI
□ NO
□ NON E' NECESSARIO (specificare):_____

- Sono conservati i log amministratore di sistema secondo le caratteristiche indicate nel provvedimento novembre 2008?

□ SI
□ NO
□ NON E' NECESSARIO (specificare):_____

18) E' prevista una policy che gestisce la comunicazione tempestiva al Titolare in caso di arrivo/cambio di mansione/dimissione degli amministratori che accedono ai dati dello stesso?

□ SI (specificare): _____
□ NO
□ NON E' NECESSARIO (specificare):_____

19) In caso di interruzione del rapporto è possibile cancellare/anonimizzare i dati personali del Titolare in modalità sicura?

□ SI IMMEDIATAMENTE
□ NO
□ SOLO SUCCESSIVAMENTE PERCHE' _____ (es sono presenti nel piano di back up del Responsabile e saranno conservati per x tempo indicare il termine di conservazione)

Altro specificare:

_____
_____

20) Avete previsto una procedura di data retention dei dati personali del Titolare e la loro cancellazione/anonimizzazione sicura?

□ SI
□ NON E' NECESSARIO (specificare):_____
□ NO

Se SI indicare la procedura:

_____

21) Avete previsto una procedura per la gestione dei diritti degli interessati anche in qualità di Responsabile del trattamento che prevede la tempestiva comunicazione dell'esercizio al Titolare?

□ SI
NO

Altro specificare:

_____
_____

22) Il servizio erogato al Titolare prevede l'esercizio della portabilità del dati?

- □ SI (allegare documentazione)
- □ NON E' NECESSARIO (specificare):_____
- □ NO

23) Avete previsto un sistema per gestire l'accesso sicuro agli archivi contenenti dati personali del Titolare?

- □ SI
- □ NO

24) I sistemi su cui sono conservati i dati del Titolare si trovano in azienda oppure anche presso fornitori esterni in outsourcing?

- □ SI
- □ NO
- □ Se SI indicare il luogo dove sono ubicati:

  _____

25) Il Servizio erogato per conto del Titolare prevede il trasferimento dei dati in paesi Europei o Extra europei?

- □ SI
- □ NO

Se SI indicare lo/gli Stato/i:

_____

26) Il Servizio erogato prevede la necessità di ricorrere a Sub Responsabili e sono stati comunicati ed autorizzati dal Titolare prima di procedere all'eventuale conferimento dell'incarico?

- □ SI
- □ NO

Se SI completare la tabella

Cognome Nome /Ragione Sociale	**Partita Iva**	**Tipologia di Servizio erogato**	**Stato di conservazione dei dati**

27) I Sub Responsabili hanno sottoscritto un contratto o altro atto giuridico a norma del GDPR che prevede gli stessi obblighi in materia di protezione dei dati contenuti nel contratto sottoscritto con il Titolare e gli obblighi di segnalazione tempestiva in caso di violazione dei dati (data breach) ?

- SI
- NO

NON E' NECESSARIO (specificare):_____

28) È stata accertata (ed è verificata almeno con cadenza annuale secondo i termini della nomina) l'adeguatezza delle misure tecniche e organizzative di ogni Sub Responsabile rispetto ai requisiti previsti dalla Normativa Privacy, anche tramite sistemi diversi di conformità? (barrare N/A nel caso non vengano utilizzati sub responsabili)

- SI
- NO
- N/A

29) In caso di violazione dei dati personali (Data Breach), è stato creata procedura che preveda gestione, comunicazione, verifica, registro delle violazioni anche in qualità di Responsabile del trattamento?

- SI
- NO

Se SI indicare nome procedura, edizione, revisione e data:

_____
_____

30) Quante violazione di "tipo 1" sono presenti nel registro delle violazione dei dati personali ai sensi dell'Art. 33 punto 5)? ("tipo 1": violazione che devono essere registrate ma non comunicate nè all'Autorità Garante né agli interessati)

- Da 1 a 10
- Da 11 a 50
- Oltre 50
- Nessuna

31) Esiste una procedura per il salvataggio dei dati personali e l'individuazione della figura responsabile per la verifica dei back up che permette di assicurare la disponibilità del dato?

- SI
- NON E' NECESSARIO (specificare):_____
- NO

Se SI indicare i riferimenti:

_____

32) Esiste una procedura per la dismissione sicura degli asset contenenti dati/informazioni del Titolare?

- ☐ SI
- ☐ NO

Se SI indicare i riferimenti, nome procedura, edizione, revisione e data:

_____
_____

Le informazioni rilasciate sono aggiornate alla data di sottoscrizione del presente documento. Qualsiasi variazione successiva dovrà essere comunicata all'indirizzo mail _____ entro 10 gg. lavorativi decorrenti dalla modifica, aggiornando il presente documento

Luogo e data

Timbro e firma del Fornitore/Responsabile del trattamento