**ALLEGATO B: PRIVACY BY DESIGN E BY DEFAULT**

Da compilare:

* da parte del fornitore aggiudicatario di gara
* da parte del fornitore che offre prodotto in dimostrazione

In quanto titolare del trattamento, l’Azienda Ospedaliera, per essere in regola con le vigenti normative in materia di Privacy è tenuta a valutare la protezione dei dati personali sin dalla progettazione relativamente a qualunque attività di trattamento e a dimostrare di aver preso in considerazione e di aver adottato tutte le misure di sicurezza ritenute necessarie per la protezione dei dati personali trattati e di aver valutato i rischi connessi all’utilizzo dello Strumento.

Pertanto, dove il rapporto contrattuale preveda la fornitura di un dispositivo medico, software o comunque un servizio **che tratti dati personali** è obbligatorio che la società proponente comunichi le misure di sicurezza tecniche ed organizzative poste in essere a protezione dei dati personali affinché l’A.O.U. Policlinico Consorziale di Bari possa correttamente compilare il proprio registro dei trattamenti.

Pertanto, qualora lo Strumento (dispositivo medico/software/servizio) tratti in qualsivoglia maniera dati personali, si prega di rispondere alle seguenti domande:

**Tipologia\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Produttore\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Modello\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. Si prega di indicare i dati personali che verranno trattati dallo Strumento indicando il ciclo di vita del dato dalla memorizzazione, agli eventuali trasferimenti, la durata, fino alla distruzione e le modalità del trattamento (art. 30 G.D.P.R.).
2. la denominazione del trattamento da effettuare attraverso lo “strumento” (ad esempio: gestione sanitaria dei pazienti);
3. le categorie di soggetti interessati (ad es.: pazienti, dipendenti, ecc.);
4. le categorie di dati personali trattati (ad es.: dati di contatto, categorie particolari di dati);
5. le categorie di destinatari a cui i dati possono o devono essere comunicati attraverso l’utilizzo dello Strumento (ad esempio: subresponsabili e/o Enti previsti dalla legge);
6. i Paesi stranieri verso cui i dati potrebbero essere trasferiti (ad es.: dati memorizzati in cloud o utilizzo di portale web con hosting al di fuori dell’Unione Europea);
7. le garanzie adottate a tutela del trasferimento internazionale dei dati personali (ad esempio: Clausole contrattuali standard, Privacy Shield, Binding Corporate Rules);
8. il periodo di conservazione dei dati (ad esempio: 10 anni o comunque per il tempo necessario a tutelare i diritti legali del titolare);
9. le misure di sicurezza fisiche, organizzative e tecniche adottate per la protezione dei dati;
10. le misure tecniche adottate in caso di trasmissione in rete delle informazioni;
11. la fonte dei dati personali (ad esempio: se conferiti dall’interessato o acquisiti da fonti esterne e/o da terzi);
12. la necessità o meno di una valutazione d’impatto sulla protezione dei dati.
13. Si prega di dichiarare se i dati richiesti dallo Strumento siano calibrati in base alla finalità del trattamento (principio di minimizzazione).
14. Si prega di dichiarare se il Fornitore, in qualità di Responsabile del trattamento, si avvalga di subresponsabili per i trattamenti afferenti al contratto di appalto, e se i rapporti con gli stessi siano correttamente regolamentati.
15. Si prega di dichiarare se lo Strumento effettui trasferimenti di Dati all’interno o al di fuori dell’Unione Europea indicando i destinatari e i rapporti con gli stessi (contitolari, subresponsabili).
16. Si prega di dichiarare le misure di sicurezza implementate a protezione dei dati presenti sullo Strumento (art. 32 G.D.P.R.).
17. Si prega di indicare le procedure di gestione di incidenti informatici e/o perdita, le attività predisposte per la cancellazione a fine vita/periodo di prova dei Dati Personali presenti sullo Strumento.
18. Si prega di indicare le misure di aggiornamento e continuità in merito alla sicurezza dello Strumento (ad es. aggiornamenti del firmware).
19. Si prega di allegare eventuali certificazioni specifiche in materia di protezione dati relative allo strumento inclusa una eventuale valutazione di impatto privacy (PIA).