**CHECKLIST GDPR DI BEREAL ITALIA**

**1. Raccolta e gestione del consenso**

Il consenso è richiesto in modo esplicito (non pre-spuntato)? → **Presente**

È possibile revocare il consenso con facilità? → **Non presente**

Il consenso è granulare (separato per diverse finalità)? → **Non specificato chiaramente**

Esiste un sistema per documentare quando e come è stato ottenuto il consenso? → **Non presente**

Per i minori: è implementato un sistema di verifica dell'età e consenso parentale? → **Non menzionato**

**2. Informativa sulla privacy**

L'informativa è facilmente accessibile? → **Presente**

È scritta in linguaggio chiaro e comprensibile? → **Presente**

Contiene tutte le informazioni obbligatorie:

* Identità e contatti del titolare del trattamento → **Presente**
* Contatti del DPO (se presente) → **Presente**
* Finalità del trattamento e base giuridica → **Presente**
* Categorie di dati personali raccolti → **Presente**
* Destinatari dei dati → **Presente**
* Eventuali trasferimenti verso paesi terzi → **Presente**
* Periodo di conservazione dei dati → **Presente**
* Diritti dell'interessato → **Presente**
* Diritto di proporre reclamo all'autorità di controllo → **Presente**
* Se il conferimento dei dati è obbligatorio o facoltativo → **Presente**
* Esistenza di processi decisionali automatizzati/profilazione → **Non menzionato**

**3. Diritti degli interessati**

Esiste una procedura per gestire le richieste di:

* Accesso ai dati → **Presente**
* Rettifica dei dati → **Presente**
* Cancellazione (diritto all'oblio) → **Presente**
* Limitazione del trattamento → **Presente**
* Portabilità dei dati → **Presente**
* Opposizione al trattamento → **Presente**

**4. Misure di sicurezza tecnica**

I dati sono protetti con crittografia (in transito e a riposo)? → **Non presente**

Esiste un sistema di autenticazione a più fattori? → **Non menzionato**

I diritti di accesso ai dati seguono il principio di minimo privilegio? → **Presente**

Sono implementati sistemi di logging per tracciare gli accessi ai dati? → **Presente**

Esistono procedure di backup regolari? → **Non presente**

Viene effettuata una pseudonimizzazione o anonimizzazione dei dati quando possibile? → **Non menzionato**

**5. Gestione dei data breach**

Esiste una procedura documentata per rilevare e gestire le violazioni? → **Presente**

È chiaro chi deve essere notificato internamente in caso di violazione? → **Non presente**

Esiste un template per notificare il Garante entro 72 ore? → **Non menzionato**

Sono definiti i criteri per valutare quando notificare gli interessati? → **Non menzionato**

Esiste un registro delle violazioni? → **Non menzionato**

**6. Trasferimenti internazionali di dati**

Sono identificati tutti i trasferimenti verso paesi extra-UE? → **Non presente**

È documentata la valutazione dei rischi per ogni trasferimento? → **Non menzionato**

**7. Registri delle attività di trattamento**

Esiste un registro completo e aggiornato dei trattamenti? → **Presente**

Per ogni trattamento sono identificati:

* Finalità → **Presente**
* Categorie di interessati e di dati → **Presente**
* Categorie di destinatari → **Presente**
* Trasferimenti verso paesi terzi → **Presente**
* Termini di cancellazione → **Presente**
* Misure di sicurezza adottate → **Presente**

**8. Privacy by Design e by Default**

La protezione dei dati è considerata fin dalla progettazione? → **Presente**

Sono raccolti solo i dati strettamente necessari (minimizzazione)? → **Presente**

I periodi di conservazione sono limitati al necessario? → **Presente**

**9. Cookie e tecnologie di tracciamento**

I cookie di profilazione sono attivati solo dopo consenso esplicito? → **Presente**

È possibile rifiutare i cookie non essenziali con la stessa facilità con cui li si accetta? → **Presente**

La cookie policy è chiara e completa? → **Non presente**

Sono implementate corrette misure tecniche (es. durata dei cookie limitata)? → **Non menzionato**