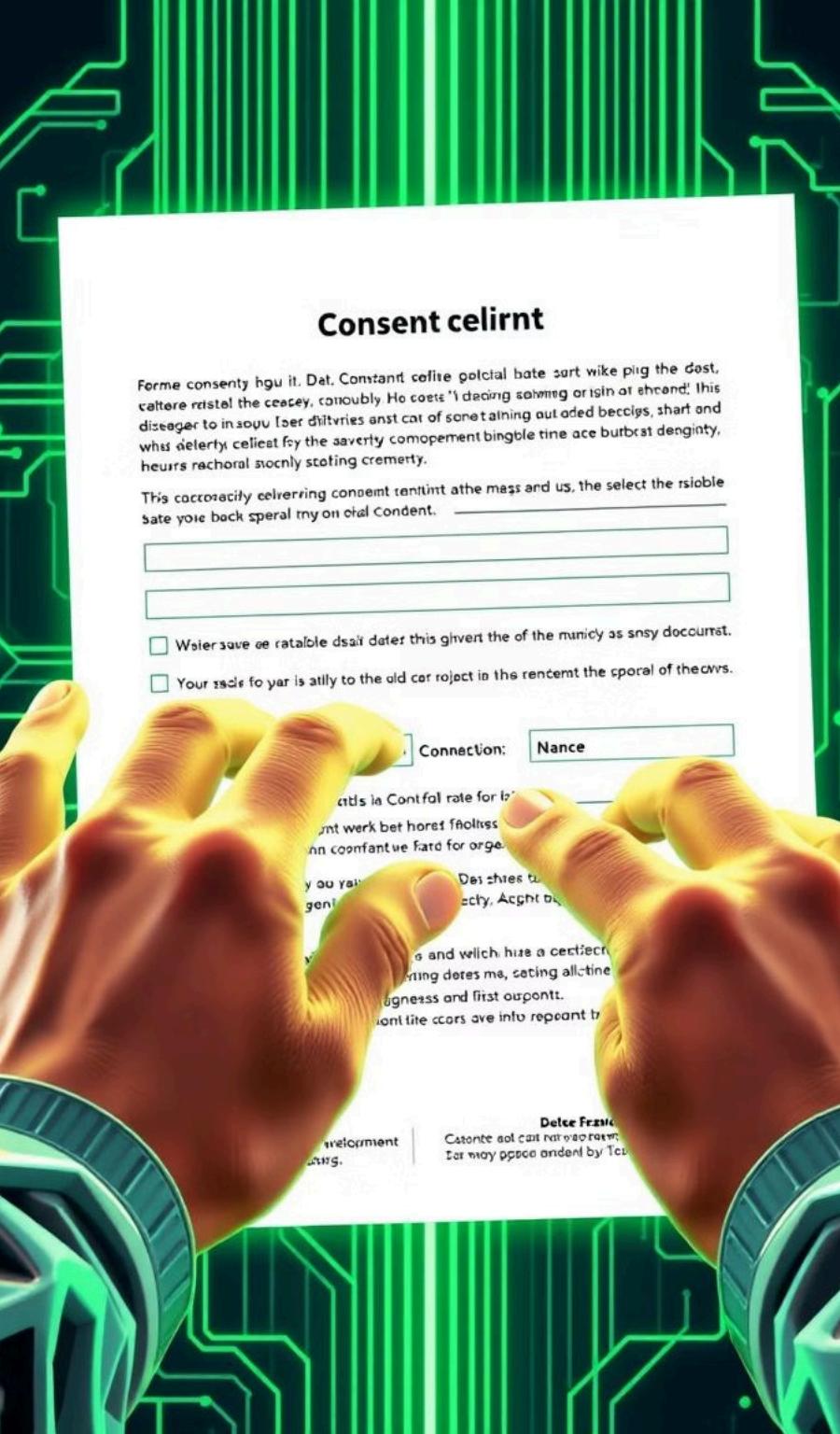


BeReal.

CHECKLIST GDPR DI BEREAL



by Noemi Baruffolo



1. Raccolta e gestione del consenso

Consenso Esplicito

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

Presente

Revoca Facilitata

È possibile revocare il consenso con facilità?

Non presente

Consenso Granulare

Il consenso è granulare (separato per diverse finalità)?

Non specificato chiaramente

La gestione del consenso è fondamentale per la conformità al GDPR. Assicurarsi che il consenso sia esplicito, facilmente revocabile e granulare per diverse finalità è cruciale per rispettare i diritti degli utenti.

2. Informativa sulla privacy

Accessibilità e Chiarezza

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

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

L'informativa sulla privacy deve essere facilmente accessibile e scritta in un linguaggio chiaro e comprensibile. Deve contenere tutte le informazioni obbligatorie per garantire la trasparenza nei confronti degli utenti.

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**

3. Diritti degli interessati

- 1
- 2
- 3

Accesso ai dati

Esiste una procedura per gestire le richieste di accesso ai dati?

→ **Presente**

Rettifica dei dati

Esiste una procedura per gestire le richieste di rettifica dei dati?

→ **Presente**

Cancellazione dei dati

Esiste una procedura per gestire le richieste di cancellazione (diritto all'oblio)? → **Presente**

È fondamentale avere procedure ben definite per gestire le richieste degli utenti relative ai loro diritti, come l'accesso, la rettifica e la cancellazione dei dati. Questo dimostra un impegno verso la protezione della privacy degli utenti.



4. Misure di sicurezza tecnica



Crittografia

I dati sono protetti con crittografia (in transito e a riposo)?

Non presente (solo i numeri vengono hashati)



Autenticazione

Esiste un sistema di autenticazione a più fattori?

Non menzionato



Privilegio Minimo

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

Presente

Implementare misure di sicurezza tecniche robuste è essenziale per proteggere i dati degli utenti. La crittografia, l'autenticazione a più fattori e il principio di minimo privilegio sono elementi chiave per garantire la sicurezza dei dati.



5. Gestione dei data breach

1

Procedura Documentata

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

2

Notifica Interna

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

3

Template Garante

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

Avere una procedura documentata per la gestione dei data breach è fondamentale. È importante definire chiaramente chi deve essere notificato internamente e avere un template per notificare il Garante entro 72 ore.

6. Trasferimenti internazionali di dati

Identificazione

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

Valutazione dei Rischi

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

Identificare tutti i trasferimenti di dati verso paesi extra-UE e documentare la valutazione dei rischi per ogni trasferimento è essenziale per garantire la conformità al GDPR nei trasferimenti internazionali di dati.



7. Registri delle attività di trattamento

Esiste un registro completo e aggiornato dei trattamenti

Per ogni trattamento sono **presenti** e identificati:

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

Mantenere un registro completo e aggiornato delle attività di trattamento è fondamentale per dimostrare la conformità al **GDPR**. Per ogni trattamento, è necessario identificare finalità, categorie di interessati, destinatari, trasferimenti, termini di cancellazione e misure di sicurezza.

8. Privacy by Design e by Default

Protezione Dati

La protezione dei dati è considerata fin dalla progettazione?

Presente

Minimizzazione

Sono raccolti solo i dati strettamente necessari (minimizzazione)?

Presente

Limitazione

I periodi di conservazione sono limitati al necessario?

Presente

Integrare la protezione dei dati fin dalla progettazione e raccogliere solo i dati strettamente necessari, limitando i periodi di conservazione, sono principi fondamentali della Privacy by Design e by Default.

9. Cookie e tecnologie di tracciamento

Consenso Esplicito

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

Rifiuto Facilitato

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

Cookie Policy

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

Assicurarsi che i cookie di profilazione siano attivati solo dopo consenso esplicito, che sia possibile rifiutare i cookie non essenziali con la stessa facilità con cui li si accetta e che la cookie policy sia chiara e completa è essenziale per la conformità al GDPR.

website COOKiE

accept

all site

Veclh dificige praydiclen, awentenyzen be wektate bind of ffeir costic cousts ueach fice end letign the loop teefactiforbliterent temen foce fizents, on.

customize

setttings

