Analisi GDPR

Made in Lab accompagna le Aziende nell'adeguamento immediato dei propri processi interni al nuovo Regolamento Europeo 679/2016 – GDPR, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

In tale contesto Made in Lab pone priorità e precedenza alla privacy degli utenti, potenziando la comunicazione aziendale interna attraverso programmi di formazione specifica affinché tutto il personale che ha accesso e gestisce i dati personali degli utenti sappia correttamente entro quali limiti poter svolgere la propria attività.

Made in Lab applica il concetto di privacy by design, un punto cardine del GDPR, che stabilisce il principio per cui le misure di salvaguardia dei dati personali debbano essere pianificate sin dalla progettazione dei processi aziendali. A tale fine offre uno staff interdisciplinare per garantire l'implementazione di misure adeguate di protezione e l'adempimento degli obblighi legali previsti dal GDPR, mediante mappatura delle operazioni di trattamento dei dati personali in un apposito registro.

Inoltre applica il concetto di accoutability, adottando politiche e misure idonee a garantire la conformità del trattamento allo stesso Regolamento e rendendo possibile verificare l'attuazione di meccanismi pratici nelle fattispecie concrete.

Preferisci il modulo cartaceo? Puoi reperire il modulo da questo link.

Nome Azienda

Nome referente

Ruolo aziendale

Telefono

Email aziendale

Indirizzo

- **Dov'è la sede del Titolare[1] del trattamento?**

  ○ Unione Europea, ○ Extra Unione Europea

- **[solo in caso di risposta "Extra Unione Europea]**

C’è un Rappresentante[1] del Titolare del trattamento?

Si No

- **Sono presenti più Titolari[1] del trattamento?**

Si No

- **Dove si trovano gli Interessati[2]?**

Persone fisiche in Unione Europea Persone fisiche Extra Unione Europea

- **I dati vengono trasferiti al di fuori della UE?**

Sì No

- **Qual è la locazione di server e database?**

Unione Europea Extra Unione Europea

- **I dati vengono memorizzati sul cloud?**

Si No

- **I dati vengono memorizzati su un server/database interno all’azienda o di proprietà di terze parti?**

Sì No

- **Quali categorie di dati sono raccolti?[3/4]**

Dati personali[2] Particolari categorie di dati[3] Dati Giudiziari[4] Dati biometrici o genetici[5]

---

[1] Ai sensi dell’art. 4, 17) del GDPR il Rappresentante del Trattamento è la persona fisica o giuridica stabilita nell'UE, designata dal titolare o dal responsabile, che li rappresenta per quanto riguarda i rispettivi obblighi.

[2] Ai sensi dell’art. 4 del GDPR sono dati personali nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici dell’identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

[3] Ai sensi dell’art. 9 del GDPR sono particolari categorie di dati i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

[4] Sono dati che rivelano l’esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad es. i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione).

[5] Ai sensi dell’art. 4 del GDPR i dati biometrici sono dati ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica quali l'immagine facciale o i dati dattiloscopici; i dati genetici sono relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che

- **I dati raccolti sono riferibili a quali categorie di interessati?**

  ☐ Dipendenti e/o collaboratori ☐ nucleo familiare di dipendenti ☐ Clienti ☐ Fornitori ☐ Possibili futuri clienti ☐ altri soggetti terzi/terze parti

- **Qual è la provenienza dei dati raccolti?**

  ☐ Dati raccolti direttamente dall'interessato ☐ Dati raccolti da terze parti ☐ Dati raccolti automaticamente ☐ Dati raccolti da pubblici elenchi o registri

- **È nominato un Responsabile del Trattamento[5](o più di uno)?**

  ○ Sì ○ No

- **Sono nominate persone autorizzate al trattamento (Incaricati ex art. 30 D.Lgs. 196/2003 - Codice Privacy)?[6]**

  ○ Sì ○ No

- **Le persone autorizzate al trattamento hanno ricevuto idonea formazione?**

  ○ Sì ○ No

- **Le persone autorizzate al trattamento hanno ricevuto credenziali di autenticazione?**

  ○ Sì ○ No

- **È nominato il DPO? [7]**

  ○ Sì ○ No

- **È stato predisposto il registro trattamenti?[8]**

  ○ Sì, ed è obbligatorio ○ Sì, non è obbligatorio ○ No

- **[in caso di risposta affermativa]**

  Il registro dei trattamenti è regolarmente aggiornato?[8]

  ○ Sì ○ No

---

forniscono informazioni sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

- **Esiste una procedura per gestire eventuali violazioni dei dati personali?**

  ○ Sì ○ No

- **Ci sono misure tecniche e organizzative che consentono di identificare i dati, cancellarli, modificarli e limitarne l'utilizzo (es. pseudonimizzazione, minimizzazione, password, antivirus, firewall, segregazione accessi)?**

  ○ Sì ○ No

- **Ci sono misure tecniche e organizzative per la conservazione dei dati (es. armadi chiusi a chiave, allarmi)?**

  ○ Sì ○ No

- **Viene eseguita la DPIA9, Valutazione di Impatto Privacy**

  ○ Sì, ed è obbligatorio ○ Sì, non è obbligatorio ○ No

- **È prevista e disponibile idonea informativa al trattamento dei dati personali?**

  ○ Sì ○ No

- **Qual è la base giuridica del trattamento?**

  ○ Adempimenti contrattuali ○ Obblighi di legge ◉ Interesse legittimo prevalente ○ Consenso interesse pubblico o esercizio di pubblici poteri

- **Quali sono le finalità del trattamento?**

  ☐ Controllo sul luogo di lavoro ☐ Vendita o comunicazione a terzi dei dati raccolti ☐ Comunicazioni commerciali e promozionali ☐ Profilazione

- **L'Azienda raccoglie e tratta i dati personali ai fini sopra indicati per conto di qualcun altro?**

  ○ Sì ○ No

- **È prevista la raccolta del consenso, ove necessario?**

  ◉ Sì, i consensi sono raccolti e conservati ○ Sì, i consensi sono raccolti ma non conservati ○ No, non viene raccolto alcun consenso

- **Qual è il tempo di conservazione dei dati?**

  ○ È previsto un termine massimo di conservazione ● Non è previsto alcun termine ○ Non è previsto alcun termine, ma sono previsti i criteri per individuarlo

- **Sono previsti strumenti applicativi per garantire i diritti dell'interessato?[10]**

  ○ Sì ○ No

- **L'azienda ha un sito web?**

  ○ Sì, un sito informativo ○ Sì, un sito e-commerce B2B ○ Sì, un sito e-commerce B2C

- **L'azienda svolge o ha intenzione di svolgere attività di marketing?**

  ○ Sì ○ No

- **L'azienda svolge o ha intenzione di svolgere attività di marketing online?**

  ○ Sì ○ No

  [in caso di risposta affermativa: descrivere brevemente la procedura adottata nella specifica attività di marketing online per la raccolta e il trattamento di dati personali?]

- **È presente un sistema di protezione dei dati?**

  ○ Sì, è previsto un sistema di protezione hardware ○ Sì, sistemi di protezione firewall ○ Sì, sistemi di protezione software ○ No, non è presente alcun sistema di protezione

- **È previsto un sistema di accessi ai dispositivi?**

  ○ Si accede con password ○ Si accede con dispositivo di autenticazione ○ Si accede attraverso una caratteristica biometrica (impronta digitale) ○ Nessuna delle precedenti risposte

- **È previsto un sistema di gestione password centralizzato?**

  ○ Sì ○ No

- **Qualora una persona autorizzata al trattamento lasci il proprio ruolo cosa accade?**

  ○ I suoi accessi vengono rimossi ○ I suoi accessi vengono conservati per un certo periodo ○ I suoi accessi vengono riutilizzati

- **Sono presenti persone autorizzate al trattamento (Responsabili interni ex art. 29 D.Lgs. 196/2003)?[6]**

  ○ Sì ○ No

- **È presente una persona autorizzata al trattamento per la funzione IT (Responsabile interno ex art. 29 D.Lgs. 196/2003)?**

  ○ Sì ○ No

- **È prevista una procedura di disaster recovery per ripristinare la disponibilità dei dati in caso di incidente fisico o tecnico?**

  ○ Sì ○ No

- **Sono previste procedure di back up dei dati?**

  [ ]

- **È previsto un sistema di gestione sicurezza client?**

  ○ Si, sistemi di sicurezza antivirus ○ Si, sistemi di sicurezza anticriptolocker ○ No

- **È previsto un sistema di gestione sicurezza del server?**

  ○ Si, sistema di sicurezza. ○ No

- **Il database è criptato?**

  ○ Sì ○ No

- **Il sistema operativo e i software vengono aggiornati?**

  ○ Sì ○ No

- **Sono previsti interventi di manutenzione software e hardware programmati?**

  ○ Sì, a cadenza almeno semestrale ○ Sì, annualmente ○ No

- **Le persona autorizzata al trattamento (dipendenti o collaboratori esterni) utilizzano dispositivi:**

[6] Il GDPR ha eliminato la figura del responsabile interno riqualificando lo stesso come "persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare". Il Responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica o altro organismo che tratta dati personali per conto del Titolare del trattamento.

☐ Computer portatili di proprietà aziendale ☐ Computer portatili di loro proprietà ☐ Computer fissi di proprietà aziendale ☐ Altro (smarphone, tablet)

- **È stato previsto un firewall per protezione perimetrale dell'azienda in manutenzione con software aggiornato e vengono eseguiti periodicamente 'penetration test' per testare la validità delle regole:**

  ○ Sì ○ No

- **Compilare i seguenti campi per risalire a uno schema di rete attuale:**

  Numero di PC:

  Numero di server:

  Numero di telefoni aziendali:

  Numero telefoni aziendali smart IOS:

  Numero telefoni aziendali smart Android:

- **È stato previsto il log di rete switch router firewall dhcp e hotspot per i guest in wifi (per quanto tempo) per prevenire malfunzionamenti:**

  ○ Sì ○ No
  Numero di mesi:

I dati raccolti da Made in Lab saranno utilizzati ai fini della produzione dell'analisi e alla redazione dell'offerta relativa all'adeguamento alle nuove normative sulla privacy GDPR e per l'invio di aggiornamenti, documenti e newsletter le cui finalità saranno sempre dedicate ad aggiornamenti e informazioni inerenti all'informazione tecnologica. Fermo restando che l'utente è il proprietario dei dati per cui potrà chiedere in ogni momento la cancellazione, i dati saranno conservati per 10 anni nel caso in cui l'offerta sia seguita da fatturazione e 3 anni nel caso in cui l'offerta non sia seguita da fatturazione. I dati raccolti non saranno ceduti a terze parti e sono protetti attraverso i più elevati standard tecnologici a protezione e tutela della privacy.

☐ Autorizzo al trattamento dei miei dati personali, ai sensi del Reg. UE 679/2016

Invia

[1] Il Titolare del trattamento è la persona fisica o giuridica che determina le finalità e i mezzi del trattamento dei dati personali.
[2] Gli Interessati sono le persone fisiche identificate o identificabili cui i dati raccolti si riferiscono.
[3]

[5]

[6] Il GDPR ha eliminato la figura dell' Incaricato al trattamento riqualificando lo stesso come "persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare", si tratta di persone autorizzate a compiere operazioni di trattamento dei dati personali che operano sotto le direttive del Titolare o del Responsabile (ad es. dipendenti, collaboratori esterni, etc..)
[7] Il Data Protection Officer o Responsabile per la protezione dei dati personali è un professionista con competenze giuridiche, informatiche, di risk management e di analisi dei processi. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda affinché siano trattati nel rispetto delle normative privacy europee e nazionali.
[8] È un registro delle attività di trattamento svolte sotto la responsabilità del Titolare o del Responsabile del trattamento. È obbligatorio per le aziende con oltre 250 dipendenti o qualora vengano trattate particolari categorie di dati (categorie particolari di

dati giudiziari, etc.) o vengano posti in essere trattamenti non occasionali che presentino un rischio per i diritti e le libertà dell'interessato. È in ogni caso un documento fortemente consigliato.

9 La DPIA o valutazione di impatto privacy è un processo volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio. E' obbligatoria quando il trattamento avviene mediante uso di nuove tecnologie e può presentare un rischio elevato per i diritti e le libertà delle persone fisiche (es. trattamento automatizzato, profilazione, il trattamento su larga scala di categorie particolari di dati personali o di dati giudiziari).[10] Il GDPR ha introdotto una serie di diritti in capo all'interessato, ai quali il Titolare del trattamento è tenuto a fornire riscontro entro 1 mese dalla richiesta di esercizio. Diventa quindi importante prevedere un processo idoneo a fornire il suddetto riscontro entro le tempistiche previste.