MODULO DI VALUTAZIONE PRELIMINARE
DELLA CONFORMITÀ AL REGOLAMENTO (UE) 2016/679 (GDPR)

Ad uso di Aziende private ed Enti pubblici

Il presente modulo costituisce uno strumento di prima valutazione, non esaustivo, dello stato di conformità dell'Organizzazione (Azienda privata o Ente pubblico) agli obblighi previsti dal Regolamento (UE) 2016/679 e dal D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018. Le risposte fornite costituiscono la base per l'individuazione delle aree di intervento prioritarie.

0. Dati identificativi dell'Organizzazione

Denominazione dell'Organizzazione:

_____

Tipologia di Organizzazione:
(selezionare l'opzione pertinente)

☐ Azienda privata ☐ Ente pubblico ☐ Altro (specificare):

_____

Settore di attività / missione istituzionale:

_____

Referente per la compilazione e ruolo:

_____

Data di compilazione:
____ / ____ / _____

1. Informazioni generali sull'Organizzazione

Qual è il fatturato annuo (Azienda privata) o il valore del bilancio/budget annuo (Ente pubblico)?
Scegliere lo scaglione che si avvicina di più

☐ Fino a 100.000 €
☐ da 100.000 € a 500.000 €
☐ da 500.000 € a 1.000.000 €
☐ da 1.000.000 € a 2.000.000 €
☐ da 2.000.000 € a 5.000.000 €
☐ oltre 5.000.000 €

Quante sedi avete?
Per sedi si intendono le sedi operative dove sono presenti dati personali di terzi, anche in forma cartacea

Numero sedi: _____

Quanti uffici avete?
Indicare solo le stanze dove sono conservati dati elettronici o cartacei

Numero uffici: _____

Quante persone operano nell'Organizzazione?
Indicare il numero totale tra dipendenti, collaboratori e personale in organico, anche senza permessi di trattamento

Numero persone: _____

Quanti sistemi di elaborazione avete?
Indicare tutti i PC presenti, server compresi

Numero sistemi: _____

Disponete già delle informative complete per la raccolta dei dati e, ove necessario, per l'acquisizione del consenso?

Per "complete" si intendono quelle già a norma GDPR, con tutti gli elementi richiesti dalla legge

☐ Sì ☐ No

2. Misure di sicurezza informatica

Che tipo di antivirus utilizzate?

☐ Nessun antivirus
☐ Antivirus gratuito
☐ Antivirus commerciale
☐ Antivirus centralizzato
☐ Antivirus centralizzato con monitoraggio attività file
☐ Antivirus centralizzato con gestione delle patch di aggiornamento
☐ Antivirus centralizzato con modalità protetta per operazioni bancarie
☐ Antivirus centralizzato con MDM - Mobile Device Management
☐ Antivirus centralizzato con DLP - Data Loss Prevention

Che tipo di firewall utilizzate?

☐ Nessun firewall
☐ Firewall software
☐ Firewall hardware

Avete predisposto un sistema di backup automatico?

☐ Nessun sistema di backup
☐ Sistema di backup gratuito
☐ Sistema di backup locale commerciale
☐ Sistema di backup in cloud
☐ Sistema di backup ibrido (locale + cloud)

Disponete di un sistema di crittografia?

☐ Nessuna crittografia
☐ Sistema di crittografia software di dischi rimovibili
☐ Sistema di crittografia software di dischi fissi e mobili

Utilizzate dispositivi mobili USB?

☐ Dispositivo USB semplice
☐ Chiavette USB con codice
☐ Chiavette USB con lettore di impronta digitale

3. Tecnologie utilizzate e servizi Cloud

Sezione dedicata alla ricognizione, a livello generale, delle tecnologie e dei servizi digitali (anche di terze parti) utilizzati per il trattamento dei dati personali.

L'Organizzazione utilizza soluzioni Cloud per il trattamento o la conservazione di dati personali?

☐ Sì ☐ No ☐ Non so / Da verificare

Che tipologia di soluzioni tecnologiche/Cloud utilizzate?

Scelta multipla, indicare tutte quelle pertinenti

- ☐ Cloud pubblico (es. servizi forniti da provider esterni)
- ☐ Cloud privato / infrastruttura dedicata
- ☐ Soluzione ibrida (locale + Cloud)
- ☐ Applicazioni e software as a service (SaaS) di terze parti
- ☐ Sistemi on-premise (infrastruttura interna, senza Cloud)
- ☐ Strumenti di intelligenza artificiale o automazione dei processi
- ☐ Altro (specificare):

_____

I fornitori di servizi Cloud o tecnologici che trattano dati per conto dell'Organizzazione sono stati nominati Responsabili del trattamento ai sensi dell'art. 28 GDPR?

☐ Sì ☐ No ☐ Non so / Da verificare

I dati personali vengono trasferiti o conservati anche al di fuori dell'Unione Europea (es. server o assistenza in Paesi extra-UE)?

☐ Sì ☐ No ☐ Non so / Da verificare

Sono state verificate le misure di sicurezza tecniche e organizzative adottate dai fornitori esterni (data center, Cloud provider, gestori di software gestionali, ecc.)?

☐ Sì ☐ No ☐ Non so / Da verificare

È stato censito l'elenco completo dei fornitori tecnologici e delle piattaforme digitali che trattano dati personali per conto dell'Organizzazione?

☐ Sì ☐ No ☐ Non so / Da verificare

4. Gestione dei dati cartacei

Trattate anche dati in formato cartaceo?

☐ Sì ☐ No

Qual è la gestione documentale cartacea dei dati?

Tipologia, scelta multipla

- ☐ Contenitori con chiave
- ☐ Armadi con chiave
- ☐ Contenitori senza chiave
- ☐ Armadi senza chiave
- ☐ Armadi ignifughi
- ☐ Armadi blindati
- ☐ Armadi blindati ignifughi
- ☐ Scaffalature a vista
- ☐ Sistema di allarme

Cosa avete predisposto in caso di interruzione di corrente?

- ☐ Nessun gruppo di continuità
- ☐ Gruppi di continuità (UPS)

5. Soggetti autorizzati al trattamento

Per "soggetti autorizzati" si intende ogni persona che, a vario titolo e livello, ha il permesso di trattare dati dell'Organizzazione sia in forma elettronica che cartacea (personale interno, collaboratori, dipendenti pubblici).

Quanti soggetti autorizzati al trattamento avete?

Numero: _____

I soggetti autorizzati sono stati formati con sessioni di formazione sulla privacy dimostrabili?

☐ Sì ☐ No

È stata consegnata loro la policy informatica?

☐ Sì ☐ No

Sono stati autorizzati con atto formale/nomina firmata e mansionario?

☐ Sì ☐ No

Sareste in grado di fornire velocemente un elenco di tutti i soggetti autorizzati con i relativi permessi per ogni trattamento?

☐ Sì ☐ No

Avete provveduto a nominare il Responsabile della Protezione dei Dati (RPD/DPO)?

Per gli Enti pubblici la nomina del DPO è obbligatoria ai sensi dell'art. 37 GDPR

☐ No, e non ho documentato le motivazioni

☐ No, ma ho già documentato le motivazioni

☐ Sì, ho nominato il DPO

6. Registro dei trattamenti

L'art. 30 del Regolamento (UE) 2016/679, e in particolare il par. 4, prevede che, su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare o del responsabile, mettano il registro dei trattamenti a disposizione dell'autorità di controllo.

L'autorità di controllo (il Garante per la protezione dei dati personali) è l'ente pubblico titolato a richiedere la disponibilità del registro al fine di esaminarlo.

L'obbligo di redazione e adozione del registro non è generale per le sole imprese: il par. 5 dell'art. 30 esclude le imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento presenti un rischio per i diritti e le libertà dell'interessato, non sia occasionale o riguardi categorie particolari di dati (art. 9) o dati relativi a condanne penali e reati (art. 10).

Per gli Enti pubblici, secondo l'orientamento del Garante e delle Autorità europee, il registro dei trattamenti è da ritenersi sempre obbligatorio, indipendentemente dal numero di dipendenti. Anche per le realtà private di minori dimensioni se ne consiglia comunque l'adozione.

Avete preso posizione sul registro dei trattamenti?

☐ Non intendo predisporlo e non ho documentato il perché

☐ Non intendo predisporlo e ho già documentato il perché

☐ Lo voglio predisporre

☐ L'ho già predisposto

7. Trattamento di categorie particolari di dati (dati sensibili)

Se si trattano categorie particolari di dati (c.d. dati sensibili) è necessario innalzare il livello di protezione. Se tali dati sono trattati su larga scala o sono di particolare rilevanza, è necessario nominare un DPO, tenere obbligatoriamente il registro dei trattamenti e redigere una valutazione d'impatto (Privacy Impact Assessment).

L'Organizzazione tratta categorie particolari di dati (dati sensibili)?

☐ Sì ☐ No

8. Valutazione d'impatto sulla protezione dei dati (DPIA)

Il GDPR introduce la valutazione d'impatto (Data Protection Impact Assessment) relativa ai trattamenti che possono presentare un rischio elevato per i diritti e le libertà delle persone.

Pur non essendo obbligatoria per tutti i trattamenti, le Autorità europee ne raccomandano la predisposizione anche perché rafforza la reputazione dell'Organizzazione nei confronti di partner e cittadini/utenti. Si tratta di un documento che analizza le misure di sicurezza adottate, individua le criticità, definisce le mitigazioni del rischio e verifica che l'impatto del trattamento sia proporzionato e accettabile.

In relazione alla valutazione d'impatto (DPIA), cosa avete deciso?

- ☐ Non intendo predisporla e ho già documentato il perché
- ☐ Non intendo predisporla e non ho documentato il perché
- ☐ La voglio predisporre
- ☐ L'ho già predisposta

9. Data Breach

Il GDPR prevede che, in caso di furto o perdita di dati sostanziale, l'accaduto vada registrato in un apposito registro (registro delle violazioni/data breach) e che, in caso di violazione con impatto significativo, vi sia l'obbligo di comunicazione all'autorità di controllo entro 72 ore tramite apposito modulo.

Avete predisposto tali moduli e il relativo registro?

☐ Sì ☐ No

10. Videosorveglianza

In caso di sistemi di videosorveglianza — anche senza registrazione e anche nel caso di telecamere finte usate come deterrente — il GDPR richiede una serie di documenti e adempimenti: dalla eventuale richiesta alla Direzione territoriale del lavoro (o accordo sindacale), al principio di necessità, alla tipologia di impianti scelti, alle modalità di conservazione delle immagini, alla nomina del responsabile e dei soggetti autorizzati, all'informativa estesa e alla cartellonistica.

Avete un sistema di videosorveglianza?

- ☐ Non è presente alcun sistema di videosorveglianza
- ☐ È presente un sistema di videosorveglianza, ma non è presente tutta la documentazione in regola
- ☐ È presente un sistema di videosorveglianza con tutta la documentazione in regola

11. Georeferenziazione

In caso di veicoli con sistemi di rilevazione della posizione, il GDPR richiede una serie di documenti e adempimenti: dalla eventuale richiesta alla Direzione territoriale del lavoro o dall'accordo sindacale, al principio di necessità, alla tipologia di impianti scelti, alle modalità di conservazione dei dati, alla nomina del responsabile e dei soggetti autorizzati, agli adesivi informativi presenti su ogni veicolo.

È presente un sistema di georeferenziazione?

- ☐ Non è presente alcun sistema di georeferenziazione
- ☐ È presente un sistema di georeferenziazione, ma non è presente tutta la documentazione in regola
- ☐ È presente un sistema di georeferenziazione con tutta la documentazione in regola