PRONTI PER GDPR?

Il regolamento generale sulla protezione dei dati (GDPR) dell'UE rappresenta una modifica significativa rispetto ai precedenti requisiti di conformità in materia di Data Privacy.

L'informazione è un importante e prezioso asset per qualsiasi organizzazione. Possono essere utilizzati dati personali per molte ragioni diverse, ad esempio per: amministrazione del personale, fornitura di beni o servizi ai clienti, strategie di marketing, prevenzione del riciclaggio di denaro, gestione di flussi di entrate, ecc.

Il controllo e la gestione dei dati personali sono attività fondamentali per garantire e dimostrare la conformità al GDPR. La transizione al nuovo regime è impegnativa e richiede sia personale formato che risorse finanziarie adeguate: il livello di conformità pre-esistente incide ovviamente sull'entità dello sforzo necessario.

Basato su una revisione sintetica della normativa, il presente questionario può essere utilizzato da dirigenti e amministratori per valutare il livello base di conformità attualmente esistente all'interno dell'azienda.

Le domande non richiedono di entrare in specifici dettagli, ma mirano piuttosto a determinare il livello di controllo che un'organizzazione ha sulle informazioni personali gestite e sulla legittimità delle loro elaborazioni, attraverso una revisione dello stato dell'arte che dovrebbe aiutare a individuare le lacune esistenti in relazione ai nuovi requisiti del GDPR.

Il presente questionario, la cui compilazione non richiede una conoscenza approfondita del GDPR, si articola in sei sezioni:

- Sezione 1 - Gestione e governance della protezione dei dati
- Sezione 2 - Documentazione relativa alle operazioni di trattamento dei dati personali
- Sezione 3 - Gestione dei rischi per la sicurezza delle informazioni
- Sezione 4 - Gestione delle violazioni dei dati e altri incidenti
- Sezione 5 - Formazione e sensibilizzazione sulla protezione dei dati
- Sezione 6 - Data Assessment e specifiche dell'ambiente dati

Le domande possono richiedere più di una risposta, a seconda della dimensione e della struttura dell'organizzazione: imprese più grandi possono avere diverse unità di gestione dei propri clienti, sezioni HR e IT ciascuna con vari obblighi, politiche e procedure.

Il questionario è stato elaborato a partire da analoghi documenti prodotti dal Garante europeo della protezione dei dati (EDPS), nell'ambito della sua iniziativa sull'Accountability per le istituzioni dell'Unione europea.

Sezione 1 - Gestione e governance della protezione dei dati

Responsabilità al più alto livello per la valutazione (assessment) e il monitoraggio dell'attuazione, nonché per fornire evidenze della qualità dell'attuazione agli stakeholder esterni e all'Autorità Garante

Attività di protezione dei dati	**Assegnazione della responsabilità della protezione dei dati al Data Protection Officer (se del caso)** **Articoli da 37 a 39**		
Domanda	Fermo restando che l'alta direzione rimane, in ultima analisi, la responsabile della compliance, la responsabilità del controllo della conformità alle norme sulla protezione dei dati è stata formalmente attribuita ad un DPO?		
Risposte Gli esempi includono: Se è necessario un DPO, cosa è stato fatto in merito? Se non è necessario un DPO, perché no?		Evidenze Gli esempi includono: Come e da chi è stato nominato? Data della nomina? Durata dell'incarico?	
Risposta creata da:	[Denominazione unità responsabile]	Data:	

Attività di protezione dei dati	**Assegnazione delle responsabilità della protezione dei dati in tutta l'organizzazione** **Articoli 24, 32**		
Domanda	Sono state individuate le responsabilità in materia di protezione dei dati nelle unità operative, nei settori e nei ruoli specifici all'interno dell'organizzazione?		
Risposte Gli esempi includono: Quali ruoli / aree? Chi? Quali sono stati i criteri adottati? Il personale è consapevole del proprio ruolo nella protezione dei dati personali?		Evidenze Gli esempi includono: Descrizione del lavoro, organigramma, verbali	
Risposta creata da:	[Denominazione unità responsabile]	Data:	

Attività di protezione dei dati	**Comunicazione e collaborazione tra le funzioni responsabili della protezione dei dati** **Articolo 39**		
Domanda	Il DPO e il senior management comunicano e lavorano insieme per garantire la conformità alla protezione dei dati?		
Risposte Gli esempi includono: Descrizione dei meccanismi di reporting Canali di comunicazione in essere		Evidenze Gli esempi includono: Politiche e procedure adottate Descrizione del lavoro, organigramma, verbali	
Risposta creata da:	[Denominazione unità responsabile]	Data:	

Attività di protezione dei dati	**Reporting sulla gestione della protezione dei dati nell'organizzazione** **Articolo 39**		
Domanda	Il DPO fornisce con regolarità i suoi report direttamente al più alto livello del management?		
Risposte Gli esempi includono: Frequenza dei report. Linee di reporting		Evidenze Gli esempi includono: Politiche e procedure adottate Verbali di riunioni	
Risposta creata da:	[Denominazione unità responsabile]	Data:	

Sezione 2 - Documentazione relativa alle operazioni di trattamento dei dati personali

Politiche interne trasparenti di protezione dei dati e della privacy, approvate e sostenute dal più alto livello di management dell'organizzazione

Attività di protezione dei dati	**Integrazione della data protection nelle procedure di accesso ed elaborazione dei dati personali utilizzati dall'organizzazione**		
Domanda	Quali sono le politiche e procedure per la protezione dei dati personali utilizzati per finalità collegate ad attività lavorative?		
Risposte Gli esempi includono: Quali dati personali vengono elaborati? Quali politiche e procedure sono presenti? Ci sono politiche separate per diverse aree di business? Dove sono disponibili? Sono riviste e aggiornate regolarmente? Vengono applicate / seguite?		Evidenze Gli esempi includono: Politiche, procedure, orari di revisione Schedulazione della formazione del personale	
Risposta creata da:	[Denominazione unità responsabile]	Data:	

Attività di protezione dei dati	**Integrare la protezione dei dati nell'utilizzo di dispositivi IT**		
Domanda	Avete procedure e policy per la protezione dei dati personali nel caso dispositivi mobili siano utilizzati per finalità collegate ad attività lavorative?		
Risposte Gli esempi includono: Quali sono? Ci sono politiche separate per device aziendali e per BYOD? Queste politiche sono applicate e rispettate? Dove sono disponibili? Sono riviste e aggiornate regolarmente?		Evidenze Gli esempi includono: Politiche, procedure, piani di revisione, piani di formazione Schedulazione della formazione del personale	
Risposta creata da:	[Denominazione unità responsabile]	Data:	

Attività di protezione dei dati	**Integrare la protezione dei dati nell'uso delle infrastrutture IT**		
Domanda	Avete procedure e policy per la protezione dei dati personali nel caso che infrastrutture IT siano utilizzate per obiettivi personali?		
Risposte Gli esempi includono: Quali sono? Queste politiche sono applicate e rispettate? Dove sono disponibili? Sono riviste e aggiornate regolarmente?		Evidenze Gli esempi includono: Politiche, procedure, piani di revisione, piani di formazione Schedulazione della formazione del personale	
Risposta creata da:	[Denominazione unità responsabile]	Data:	

Attività di protezione dei dati	**Integrare la protezione dei dati nelle pratiche di monitoraggio delle comunicazioni fra dipendenti**		
Domanda	Avete procedure per integrare la protezione dei dati nelle pratiche di monitoraggio delle comunicazioni, come utilizzo personale di e-mail, internet e telefono?		
Risposte Gli esempi includono: Quali sono? Queste politiche sono applicate e rispettate? Dove sono disponibili? Sono riviste e aggiornate regolarmente?		Evidenze Gli esempi includono: Politiche, procedure, piani di revisione, piani di formazione Schedulazione della formazione del personale	
Risposta creata da:	[Denominazione unità responsabile]	Data:	

Sezione 3 - Gestione dei rischi per la sicurezza delle informazioni

Politiche interne trasparenti di protezione dei dati e della privacy, approvate e sostenute dal più alto livello di management dell'organizzazione

Attività di protezione dei dati	**Mantenere e aggiornare una policy per la sicurezza delle informazioni** **Art 32**		
Domanda	Avete una politica per la sicurezza delle informazioni in grado di proteggere i dati personali?		
Risposte Gli esempi includono: La policy aziendale identifica il rischio per le persone generato dai processi? Livelli di sicurezza? Livello di resilienza di sistemi e dati? Azioni che mantengono l'accesso ai dati nel caso di incidenti tecnici o fisici? Test e valutazioni periodiche delle misure adottate		Evidenze Gli esempi includono: Assessment sullo stato di sicurezza Valutazioni periodiche, policy, procedure	
Risposta creata da:	[Denominazione unità responsabile]	Data:	

Sezione 4 – Gestione dei Data Breaches e di altri incidenti di sicurezza

Attuazione di adeguate procedure per porre rimedio a scarsa conformità e violazioni dei dati.

Attività di protezione dei dati	**Mantenere e documentare un protocollo di risposta per casi di incidenti e/o violazioni della protezione dei dati** **Art. 33 e 34**		
Domanda	Avete una procedura di risposta nel caso di violazioni di dati personali?		
Risposte Gli esempi includono: Qual è? Dove è disponibile? Viene rivisto regolarmente?		Evidenze Gli esempi includono: Politiche Protocolli Procedure	
Risposta creata da:	[Denominazione unità responsabile]	Data:	

Sezione 5 - Formazione e consapevolezza della protezione dei dati

Informare e formare tutte le persone dell'organizzazione su come implementare le politiche

Attività di protezione dei dati	**Mantenere consapevolezza sulle responsabilità della protezione dei dati** **Art 5 e/o 39 se viene nominato un DPO**		
Domanda	Vengono sviluppate consapevolezza e formazione del personale sulle politiche e procedure di protezione dei dati implementate dalla organizzazione per gestire i rischi legati alla sicurezza delle informazioni?		
Risposte Gli esempi includono: Quanto frequente? Sistemi di comunicazione? Disponibilità? Viene mantenuta la documentazione dei programmi di formazione?		Evidenze Gli esempi includono: Documentazione su piani di formazione svolti e schedulati	
Risposta creata da:	[Denominazione unità responsabile]	Data:	

Sezione 6 - Data Assessment e specifiche dell'ambiente dati

Valutazione della situazione di governance dei dati sensibili

Attività di protezione dei dati	**Qualità e quantità stimata dei dati sensibili**		
Tipologia di Dati Sensibili: (anagrafici / bancari / sanitari / giuridici / …)			
Numerosità dati sensibili (% su intero repository / per ogni repository)			
Dove sono memorizzati i dati (NoSQL, RDBMS / DBMS / File System / Repositories / Cloud)			
Risposta creata da:	[Denominazione unità responsabile]	Data:	

Attività di protezione dei dati	**Pratiche in atto di protezione dei dati e di restrizione degli accessi**		
Meccanismi di protezione dei dati già implementati (SI/NO – se esistono breve descrizione)			
Esistenza di policy di accesso ai dati (SI – quante /NO)			
Modalità di accesso ai dati (applicazioni custom / packages / nativa)			
Logging di accesso (è tracciato / non è tracciato)			
Risposta creata da:	[Denominazione unità responsabile]	Data:	

Attività di protezione dei dati	**Altri elementi da valutare**		
Numerosità degli utenti per applicazione/ruolo			
Gestione del consenso (implementata – Nessuna – solo su carta)			
Riconoscimento dei dati che afferiscono ai minori (autorizzazione del genitore/tutore)			
Strumenti di Data Governance disponibili (ETL / DWH / Reporting / Analytics/…)			
Risposta creata da:	[Denominazione unità responsabile]	Data:	

Attività di protezione dei dati	**Specifiche dell'ambiente dati**

DataBase

Tipo DB	Nr. Server /SO /Core x Server	Nr. Istanze di DB	Nr. Tabelle/File	Applicazioni	Utenti
Es. Oracle	*2/Linux/8CPU*	*3*	*120*	*10*	*40*

Applicazioni

Applicazione	Tipologia	Utenti	Ruoli	Interfacce
Es. CRM	*Custom*	*20*	*3*	*15*

Risposta creata da:	[Denominazione unità responsabile]	Data:	