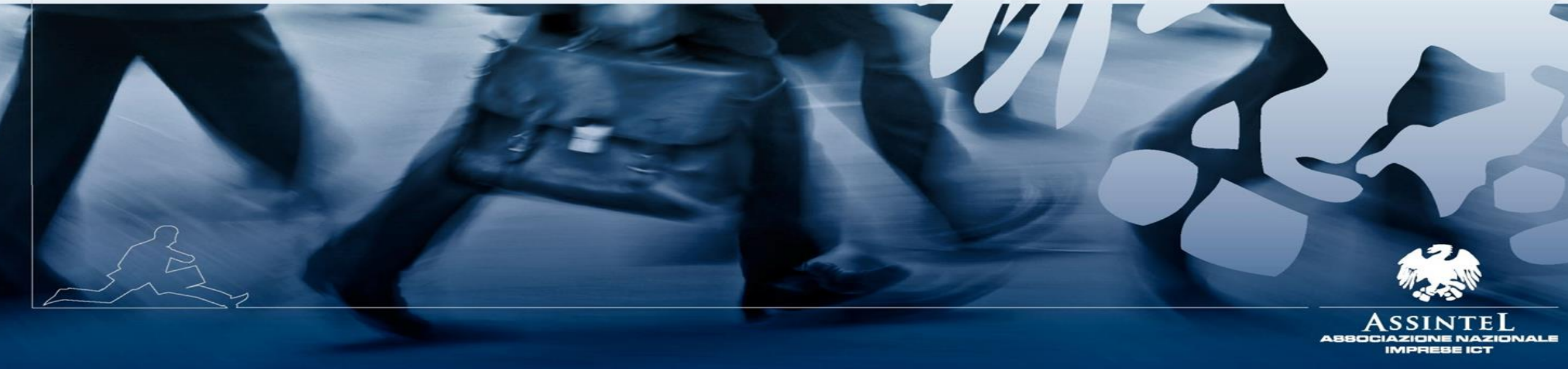
TOOL DI AUTO-VALUTAZIONE GDPR

Carlo Guastone, *Gdl Sicurezza Informatica Assintel*

Gruppo di Lavoro
SICUREZZA INFORMATICA
Assintel



ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

Sicurezza informatica e GDPR

Il Gruppo di Lavoro Sicurezza Informatica ASSINTEL - attivo sul tema della sicurezza delle informazioni aziendali, della cyber security e della protezione dei dati - è promotore di iniziative trasversali affinché possano beneficiarne le imprese di qualsiasi settore merceologico e di ogni dimensione, con particolare attenzione alle MPMI.

Tra le varie iniziative promosse ricordiamo:

- ✓ **Vademecum per la sicurezza dei dati aziendali**
- ✓ **Tool di auto-assessment** per valutare il livello di Sicurezza informatica delle PMI.
- ✓ **Predisposizione di un prototipo di auto-assessment GDPR,** per valutare i principali adempimenti che aziende dovranno realizzare entro il 25 maggio 2018 (*).

(*) Da tale data il Regolamento EU 2016/679 «General data protection regulation - GDPR», già in vigore dal 14 maggio 2016, dovrà essere applicato dalle aziende «a tutti gli effetti»

Motivazioni del Tool di aut-assessment GDPR

Aiutare le aziende a valutare l'attuale situazione interna relativa alla Privacy con particolare riferimento agli adempimenti richiesti dal GDPR:

- Normativi (es. Informative , Nomine, etc)
- Organizzativi (es. Ruoli e Responsabilità previsti da GDPR: ad es. Titolare, Responsabili, DPO se previsto, etc,)
- Tecnologici (misure tecnologiche di protezione dei dati adeguate al rischio)

Tali aspetti sono già stati approfonditi nelle precedenti presentazioni.

Le priorità del business e GDPR

GDPR non è un ostacolo allo sviluppo del business, anzi una efficace protezione dei dati personali può favorirne lo sviluppo, in particolare per le aziende commerciali che fanno e faranno sempre più utilizzo delle nuove tecnologie informatiche (es- e-commerce)

Criteri adottati

- Domande sviluppate in coerenza con le caratteristiche dell'azienda (es. n° dipendenti, trattamenti a rischio elevato, etc)
- Livello di approfondimento «ragionevole» delle domande considerando la presenza anche di aziende PMI
- Sequenza delle domande in logica di complessità crescente

- **Output: % di adempimenti già realizzati dall'azienda**

- Prototipo sviluppato in excel, usufruibile online mediante la compilazione di un questionario

76 DOMANDE

Le Sezioni del Tool di auto-assessment GDPR

L'AZIENDA e I DATI PERSONALI TRATTATI
-7 domande-

IMPATTI E RISCHI DEI TRATTAMENTI
-3 domande-

PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE
(by design e by default)
-4 domande-

REGISTRO DEI TRATTAMENTI
-3 domande-

RUOLI, RESPONSABILITA' E PROCEDURE (es. Incidenti di sicurezza)
-17 domande-

MISURE DI SICUREZZA NEI TRATTAMENTI
-13 domande-

RELAZIONI CON I FORNITORI (RESPONSABILI ESTERNI DEI TRATTAMENTI)
-4 domande-

PROFILAZIONE
(es. abitudini di consumo dei clienti, automatizzate su larga scala)
-3 domande-

CONSENSO
-4 domande-

PROVVEDIMENTI DEL GARANTE APPLICABILI
(es. videosorveglianza)
-8 domande-

Le Sezioni del Tool di auto-assessment GDPR

Assessment GDPR

1. Analisi del contesto

Numero dipendenti — < 250 | > 250

Vengono realizzate attività di profilazione sugli interessati al fine di erogare servizi a valore aggiunto? — SI | NO

Selezionare la tipologia di trattamento dei dati personali

- ○ Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico
- ◉ Le attività principali del titolare del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala
- ○ Le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati
- ○ Altro

Le Sezioni del Tool di auto-assessment GDPR

2. Assessment

/ DATA PROTECTION RISK ASSESSMENT

Anche se non obbligatorio è stato realizzato un Data Protection Impact Assessment?	SI	NO	⚠
E' stata definita ed adottata una procedura per lo svolgimento di Data Protection Inpact Assessment?	SI	NO	✓
E' svolta con regolarità una valutazione dei rischi i privacy adottando una metodologia formalizzata?	SI	NO	⚠

/ REGISTRO DEI TRATTAMENTI

E' stato realizzato un registro dei trattamenti conforme a quanto previsto dal GDPR?	SI	NO	⚠

/ RUOLI, RESPONSABILITA' E PROCEDURE

E' stato individuato e nominato un DPO?	SI	NO	⚠
Sono stati individuati Contitolari del trattamento?	SI	NO	✓

Le Sezioni del Tool di auto-assessment GDPR

3. Risultati

/ GIUDIZIO DI CONFORMITA': Sei adempiente al GDPR

/ % DI ADEMPIMENTO: %

/ INFORMAZIONI UTILI:

- Il registro dei trattamenti è obbligatorio
- La nomina del DPO è obbligatoria
- ecc.

Grazie per l'attenzione

Carlo Guastone
Vice Presidente Business development
SERNET
carlo.guastone@sernet.it
Cell. 335-5833862
www.sernet.it

Gruppo di Lavoro
SICUREZZA INFORMATICA
Assintel

@Assintel

GdL Assintel Sicurezza Informatica