AREA AFFARI LEGALI

SAPIENZA
UNIVERSITÀ DI ROMA

Al Titolare del trattamento dei dati
Università degli Studi di Roma
"Sapienza"

Alla c.a. della Magnifica Rettrice
Prof.ssa Antonella Polimeni
rettricesapienza@uniroma1.it

OGGETTO: Programma di *audit* in materia di *privacy* – anno 2022.

Introduzione.
Con la presente, il sottoscritto Responsabile della protezione dei dati personali (RPD) dell'Università degli Studi di Roma "La Sapienza" (designato con D.R. n. 409/2020) propone al Titolare del trattamento il "Programma di *audit* in materia *di privacy* - anno 2022", per la relativa approvazione.
L'art. 39 del Regolamento (UE) generale sulla protezione dei dati 2016/679 prevede, infatti, che il RPD sia incaricato di "*sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo*".

1. Organizzazione del "*Team audit* per il Regolamento generale sulla protezione dei dati"
Il "*Team audit* per il Regolamento generale sulla protezione dei dati" (di seguito, anche, "*Team*") è composto dal sottoscritto, *Lead Auditor*, dalla dott.ssa Giovanna D'Incoronato, *Auditor,* e dalla dott.ssa Anjeza Doko, *Auditor*; entrambe afferenti al Settore *Privacy* dell'Area Affari legali (ARAL); eventualmente, su indicazione del *Lead Auditor*, il *Team* si potrà avvalere, a seconda delle particolari necessità ed esigenze, di una o più specifiche componenti individuate nell'ambito del Gruppo di Lavoro "*Privacy*" (costituito con D.D. n. 3026/2020, prot. n. 46974 del 2.07.2020), oppure nell'ambito dell'Area Affari legali (ARAL), oppure nell'ambito delle Aree dirigenziali.

2. Oggettività dei controlli
Gli esiti dell'attività di monitoraggio dovranno essere oggettivamente verificabili. Conseguentemente, le verifiche saranno basate su documenti (ad esempio, registri dei trattamenti, informative, reclami, notifiche di *data breach*, accordi di contitolarità, contratti di nomina del Responsabile del trattamento, lettere di incarico, ecc.) e interviste effettuate ai soggetti auditati.
Rilevante strumento dell'attività di monitoraggio delle politiche di gestione dei dati personali è rappresentato dal Registro dei trattamenti.

Sapienza Università di Roma
Area Affari legali
Settore privacy
CF 80209930587 - PI 02133771002
p.le Aldo Moro 5
T (+39) 0649910166
www.uniroma1.it

Ad integrazione di quanto sopra precisato, potranno essere effettuate anche registrazioni sonore, fotografie o riprese video, previamente autorizzate.

3. Obiettivi

L'*audit* è finalizzato a monitorare la verifica dei principali adempimenti prescritti dalla normativa *privacy* vigente a carico dei Designati al trattamento dei dati personali, che si elencano di seguito:

a) corretta tenuta dei registri dei trattamenti (Titolare e Responsabile);
b) predisposizione e conservazione delle lettere di incarico;
c) eventuali nomine degli Amministratori di Sistema (ADS) e comunicazione dei nominativi al Centro InfoSapienza;
d) eventuali nomine dei Responsabili del trattamento *ex* art. 28 del GDPR;
e) verifica delle informative *privacy*;
f) eventuale effettuazione della Valutazione d'impatto sulla protezione dei dati (DPIA) *ex* art. 35 del GDPR;
g) verifica della conoscenza della procedura da seguire in caso di *data breach*.

4. **L'ambito dell'*audit***

Considerata la molteplicità ed eterogeneità funzionale delle Strutture di Sapienza e in generale la complessità delle funzioni esercitate dal Titolare del trattamento, si è ritenuto opportuno circoscrivere il monitoraggio annuale sulle tipologie di Strutture indicate di seguito:

- 2 Facoltà;
- 2 Dipartimenti;
- 1 Centro.

L'*audit* si concentrerà sull' obiettivo indicato al precedente punto 3.

Almeno 15 giorni prima dell'*audit*, lo scrivente comunicherà alla Struttura auditata l'avvio delle operazioni, con lettera formale contenente:

a) la data della riunione di apertura con il Responsabile della Struttura e con i collaboratori da lui individuati;
b) la definizione dei particolari obiettivi dell'*audit*;
c) il piano di *audit* (con un adeguato grado di flessibilità per consentire cambiamenti che possono rilevarsi necessari nel corso delle attività), le modalità di svolgimento, la necessaria documentazione (evidenze documentali) da sottoporre agli esami degli *auditor*.

5. Svolgimento dell'*audit* e predisposizione delle conclusioni

L'azione 8.10.a) del nuovo *Addendum* al Piano di conformità *privacy* (adottato con D.R. n. 3481/2021) prevedeva "l'attivazione dell'attività di *audit* interna" entro il 31.12.2021.

In un'ottica di continuità con la succitata azione già conclusa nel corso dell'anno 2021 e considerati i risultati delle attività di *audit* che sono state svolte nel corso dello scorso anno, il "*Team audit* per il Regolamento generale sulla protezione dei dati" procederà all'esame della documentazione richiesta, alle eventuali interviste, nonché all'osservazione delle attività di trattamento.

Qualora siano ravvisate delle “non conformità” (NC) - ovverosia il mancato rispetto della normativa di settore - e dopo averne accertato le cause, verranno fornite istruzioni per la relativa rimozione e la tempistica di intervento: seguirà, quindi, una successiva verifica di avvenuta regolarizzazione.

6. Rapporto finale

Terminate le verifiche programmate, gli esiti dell’*audit* confluiranno in un *report*, nel quale verranno accertate le non conformità emerse (con specificazione delle relative azioni correttive o preventive) e/o verranno proposte delle raccomandazioni (azioni di miglioramento); il *report,* datato e firmato dai partecipanti all’*audit* (sia del *Team*, che della Struttura auditata)*,* sarà trasmesso al Responsabile delle citate Strutture.
Le valutazioni formulate dal RPD non sono vincolanti.

7. Attuazione del programma

Completate le azioni previste dal programma annuale, il *Lead Auditor* presenterà al Titolare una relazione sull’attività complessivamente svolta e sui risultati conseguiti.

Conclusioni

Sulla base delle motivazioni esposte, si chiede l’approvazione del Programma di *audit* in materia di *privacy* - anno 2022”, al fine di poter espletare le attività pianificate.
Distinti saluti

F.to digitalmente
Il Responsabile della protezione dei dati personali
Dott. Andrea Bonomolo

Il Titolare del trattamento, VISTO il contenuto del documento, APPROVA.

F.to digitalmente
LA RETTRICE
Prof.ssa Antonella Polimeni