AREA AFFARI LEGALI

SAPIENZA
UNIVERSITÀ DI ROMA

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

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

OGGETTO: programma di *audit* – anno 2021.

Introduzione.
Con la presente, il sottoscritto Responsabile della protezione dei dati personali (RPD) dell'Università degli Studi di Roma "Sapienza" (designato con D.R. n. 409/2020, prot. n. 8931/2020 del 31.01.2020) propone, al Titolare del trattamento, il programma di *audit* relativo all'anno 2021, 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. 302672020, prot. n. 46974 del 2.07.2020),

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

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, schede di analisi del rischio per i trattamenti fondamentali, regolamenti vigenti, informative, registri, reclami, notifiche di *data breach*, accordi di contitolarità, contratti di nomina del Responsabile del trattamento, atto di autorizzazione al trattamento, ecc.) ed interviste effettuate ai soggetti auditati.
Rilevante strumento dell'attività di monitoraggio delle politiche di gestione dei dati personali è rappresentato dal Registro dei trattamenti.
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:
a) l'attività di analisi del rischio per i trattamenti fondamentali prevista nell'ambito dell'azione 8.10.b) dell'*Addendum* al Piano di conformità *privacy* di Ateneo (D.R. n. 698/2021, prot. n. 184 del 9.03.2021);
b) l'attività di verifica di *compliance* dei regolamenti vigenti prevista nell'ambito dell'azione 8.5.b) dell'*Addendum* al Piano di conformità *privacy* di Ateneo (D.R. n. 698/2021, prot. n. 184 del 9.03.2021).
L'oggetto dell'*audit*, ovviamente, non può essere considerato esaustivo e può essere, di volta in volta, integrato a seconda dello specifico contesto nell'ambito del quale vengono svolti i trattamenti.

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

Considerata la molteplicità ed eterogeneità funzionale delle Aree e Strutture di Sapienza e, in generale, la complessità delle funzioni esercitate dal Titolare del trattamento, nonché la delicatezza e maggiore pericolosità di alcuni trattamenti, e in osservanza del principio del "*risk based approach*", si è ritenuto di concentrare il monitoraggio sulle seguenti Aree e Strutture:
- per l'attività di cui al punto 3.a): tutte le Strutture di riferimento di cui ai trattamenti nn. 3 e 13 del Registro dei trattamenti, il cui livello di impatto del rischio è ritenuto "molto alto";
- per l'attività di cui al punto 3.b): le Aree dirigenziali che hanno indicato la necessità di sottoporre a verifica di *compliance* uno o più regolamenti vigenti.

L'*audit* si concentrerà su uno o più degli obiettivi citati al precedente punto 3.
Almeno 15 giorni prima dell'*audit*, lo scrivente Responsabile della protezione dei dati personali (RPD) comunicherà, all'Area o alla Struttura auditata, l'avvio delle operazioni, con lettera formale contenente:
a) la data della riunione di apertura con il Responsabile dell'Area o della Struttura e 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. 698/2021, prot. n. 18430 del 9.03.2021) prevede, "*entro il 31.12.2021*", "*l'attivazione dell'attività di audit interna*".
In attuazione della suddetta azione, 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 proposte delle raccomandazioni (azioni di miglioramento); il *report,* datato e firmato dai partecipanti all'*audit* (sia del *Team*, che dell'Area o dalla Struttura auditata), sarà trasmesso al Responsabile dell'Area o della Struttura e al Titolare, per le iniziative del caso.
Le valutazioni formulate dal RPD non sono vincolanti.

7. Attuazione del programma
Completato il 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* per l'anno 2021, 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