CONVENZIONE PER LA NOMINA DEL
RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI

Il giorno 20 del mese novembre dell'anno 2020 tra

· Regione Toscana – Giunta regionale, con sede in Firenze , Palazzo Strozzi Sacrati, Piazza del Duomo n. 10, rappresentata dall' Ing. Fabio Martelli, nella sua qualità di delegato del titolare ex dgr 585/2018 in quanto dirigente responsabile del Settore Sistemi Informativi e Tecnologie della Conoscenza. Ufficio Regionale di Statistica;

e

· Istituto Regionale per la Programmazione Economica della Toscana (IRPET) con sede in Firenze, Villa la Quiete alle Montalve, Via Pietro Dazzi n. 1, rappresentato dal dr. Stefano Casini Benvenuti, nella sua qualità di Direttore dell'IRPET.

Premesso che

- il dirigente Ing. Fabio Martelli è stato nominato con decreto n. 9521 del 01/07/2020 responsabile del trattamento per le materie afferenti al Settore Sistemi Informativi e Tecnologie della Conoscenza. Ufficio Regionale di Statistica;
-i dirigenti competenti per materia, delegati dal Titolare Regione Toscana – Giunta regionale ai sensi della dgr 585/2018, sottoscrivono con i responsabili una convenzione redatta secondo lo schema che segue, dove sono specificate finalità e durata del trattamento, tipi di dati personali e categorie di interessati, nonché obblighi del responsabile e del titolare;
- l'IRPET è in possesso dei necessari requisiti di esperienza, affidabilità e capacità tali da fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, per poter essere individuato responsabile esterno del trattamento;
- precisato che IRPET è titolare dei prodotti delle attività di ricerca effettuate autonomamente, sulla base dei risultati delle elaborazioni effettuate, ai fini dell'attuazione del suo Programma istituzionale

SI CONVIENE E SI STIPULA QUANTO SEGUE

Art. 1 – Oggetto, finalità e durata del trattamento

Oggetto della presente convenzione sono le finalità e durata del trattamento, tipi di dati personali e categorie di interessati, nonché obblighi del responsabile e del titolare del trattamento, in relazione alla nomina da parte del dirigente responsabile Ing. Fabio Martelli, nella sua qualità di delegato del titolare, dell'Istituto Regionale per la Programmazione Economica della Toscana (IRPET) come Responsabile del trattamento per l'espletamento delle attività statistiche previste dal Programma Istituzionale dell'IRPET.
Le finalità del trattamento sono esclusivamente quelle riconducibili all'espletamento delle attività affidate al Responsabile.
La presente convenzione, la cui validità è fissata in anni cinque a far data dalla sua sottoscrizione, è rinnovabile, previa adozione di atto formale, per un ulteriore quinquennio dopo la scadenza.

Art. 2- Trattamento dei dati personali

Ai sensi e per gli effetti della normativa in materia di protezione dei dati personali (Reg. UE n. 2016/679, di seguito "GDPR", nonché D. Lgs. 196/2003 da ultimo novellato dal D. Lgs. 101/2018, di seguito "Codice Privacy") ed in relazione alle operazioni che vengono eseguite per lo svolgimento delle attività previste dalla convenzione, la Regione Toscana – Giunta Regionale, in qualità di Titolare, nomina IRPET, Responsabile del trattamento, ai sensi dell'articolo 28 GDPR.

I trattamenti affidati dal Titolare al Responsabile riguardano:

dati individuali statistici prodotti nell'ambito del Sistema Statistico Nazionale (SISTAN), comprensivi anche di codice fiscale, relativi alle seguenti categorie di interessati:

- imprese
- cittadini
- famiglie ed individui
- studenti
- istituzioni
- aziende agricole

IRPET si impegna a fornire all'ufficio di statistica della Regione Toscana (oggi Settore Sistema Informativo di Supporto alle Decisioni. Ufficio Regionale di Statistica):
- tavole e pubblicazioni relative alle elaborazioni eseguite nell'ambito del programma istituzionale che fanno uso dei dati Sistan ricevuti
- note informative e descrizioni delle metodologie e dei modelli utilizzati nell'attività di elaborazione dei dati Sistan ricevuti.

I trattamenti effettuati per conto del Titolare dal Responsabile cesseranno al completamento della convenzione ovvero in caso di sua risoluzione, per qualsiasi altro motivo.
Se una disposizione del presente articolo è o diventa invalida o inapplicabile, la validità e l'applicabilità delle altre disposizioni del medesimo rimangono inalterate. In questo caso, Titolare e Responsabile concordano di adottare una disposizione che corrisponda al meglio allo scopo previsto nella disposizione non valida o agli interessi comuni.

IRPET, in quanto Responsabile, fornisce garanzie sufficienti, in particolare in termini di conoscenze specialistiche, affidabilità e risorse, per attuare misure tecniche e organizzative che soddisfino i requisiti normativi sanciti dal GDPR, dal Codice Privacy e da qualsiasi altra norma connessa inerente al trattamento dei dati personali, comprese le misure di sicurezza del trattamento, per garantire la riservatezza e la protezione dei diritti degli interessati.
IRPET, in quanto Responsabile, è tenuto ad assicurare e far assicurare ai propri dipendenti, collaboratori e responsabili ulteriori, la riservatezza ed il corretto trattamento delle informazioni, dei documenti e degli atti amministrativi, dei quali venga a conoscenza durante l'esecuzione della prestazione.
In tal senso il responsabile, si impegna a consegnare, alla firma della convenzione, al Titolare e al DPO della Giunta Regionale Toscana "il disciplinare di comportamento degli autorizzati e degli altri dipendenti" coinvolti in modo e diretto o indiretto nella esecuzione dei trattamenti svolti per conto del Titolare e delle istruzioni impartite agli autorizzati nei loro relativi ruoli.

In particolare, ai sensi dell'art. 28 GDPR, IRPET si impegna a:

- adottare e mantenere aggiornato un proprio registro dei trattamenti, concordandone la struttura e le modalità di aggiornamento, con il DPO della Giunta Regionale Toscana entro 30 giorni dalla firma della convenzione.

- Non mettere in atto, per nessun motivo, trattamenti di dati diversi da quelli autorizzati dal Titolare oggetto della presente convenzione e presenti, se sia adottato, nel registro dei trattamenti. In tal senso renderà accessibile al Titolare il registro dei trattamenti, attivati per effetto della convenzione, consentendo operazioni di consultazione, approvazione e diniego in relazione a singoli o gruppi di trattamenti.
- fornire per iscritto agli autorizzati al trattamento le necessarie istruzioni in tema;
- nominare gli autorizzati che svolgono le funzioni di"amministratore di sistema",ai sensi dei provvedimenti del Garante italiano per la protezione dei dati personali del 27/11/2008 e del 25/6/2009,conservando i relativi estremi identificativi, definendo gli ambiti di operatività ai medesimi consentiti e comunicandone al titolare l'elenco nominativo con i relativi ambiti di operatività;
- di collaborare alla eventuale redazione di DPIA su trattamenti affidati alla sua responsabilità dal Titolare;
- predisporre e trasmettere, con cadenza annuale e comunque ogni qualvolta ciò appaia necessario, al Titolare Regione Toscana – Giunta Regionale - una relazione in merito agli adempimenti eseguiti e alle misure di sicurezza adottate al fine di renderle e mantenerle sempre adeguate ed aggiornate rispetto alla evoluzione delle minacce e sulla base dei riscontri derivanti dalla registrazione continua e puntuale degli incidenti eventualmente occorsi;
- assistere e garantire il titolare del trattamento nell'evasione delle richieste e del rispetto dei tempi previsti, nei rapporti con l'Autorità Garante per la protezione dei dati personali
- Assistere il Titolare al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati ai sensi degli artt. 15 a 22 del Regolamento UE; qualora gli interessati esercitino tale diritto verso il Responsabile, quest'ultimo è tenuto ad inoltrare tempestivamente e comunque nel più breve tempo possibile, le istanze al Titolare, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei tempi prescritti
- Assistere ed assicurare la piena, fattiva e puntuale collaborazione al titolare del trattamento,ed in particolare al Security IT Manager del Titolare se nominato, nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento, della tipologia di dati trattati, delle categorie e numerosità degli interessati.
- Garantire al Titolare, su richiesta, l'accesso e la disponibilità permanente ai dati, su formati e strumenti di uso comune che ne garantiscano la fruizione da parte del titolare, consentendo in tal modo la piena continuità dei servizi oggetto del presente appalto e in modo che mai si configuri una situazione di lock in. Il titolare deve essere sempre messo in condizione di poter garantire la continuità del servizio;
- Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento deve mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre, se del caso:

> *a.la pseudonimizzazione e la cifratura dei dati personali;*
> *b.la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;*
> *c.la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;*
> d.*una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*

A tal fine si impegna ad assistere ed assicurare la piena, fattiva e puntuale collaborazione al titolare del trattamento,ed in particolare al Security IT Manager del Titolare.

- Restituire tutti i dati personali di pertinenza del Titolare, dopo che è terminata la prestazione dei servizi relativi al trattamento, cancellando le copie esistenti in proprio possesso, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati.
- il Responsabile informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. data breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità di controllo siano esclusivamente in possesso del Responsabile e/o di suoi sub-Responsabili;
- Sarà obbligo del Titolare del trattamento vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del trattamento, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile. A tal fine il Responsabile del trattamento metterà a disposizione,su richiesta del titolare del trattamento~~,~~tutte le informazioni necessarie per dimostrare il rispetto degli obblighi derivanti dal regolamento UE, agevolando il contributo alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato, ivi compresa, se necessario~~,~~ l'attività di monitoraggio e controllo da parte del DPO e del Security IT Manager (se nominato), sulle misure di sicurezza attuate e sulla loro efficacia fornendo tutta la documentazione che sarà richiesta e collaborando attivamente alle attività di rilevazione e misura.
- Comunicare al Titolare il nome ed i dati del proprio "Responsabile della protezione dei dati" (DPO), qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali (DPO) del Fornitore/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati (DPO) del Titolare
- Comunicare al Titolare, al DPO *e al Security Manager (se nominato*) il nome e i riferimenti di contatto del proprio Responsabile della sicurezza IT,
- Mettere in atto gli interventi necessari qualora l'attività di monitoraggio e controllo mettesse in evidenza punti di debolezza nelle misure e nelle tecniche adottate o qualora durante l'esecuzione della Convenzione, la normativa in materia di Trattamento dei Dati Personali generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti;
- Fornire e mantenere aggiornato il catalogo degli asset (comprese le applicazioni utente e quelle di gestione dei sistemi e degli apparati), delle minacce e delle misure di sicurezza adottate e delle loro correlazioni al fine di una agevole valutazione dei rischi in fase di DPIA. A tal fine il Titolare concorda entro 30 giorni dalla firma della convenzione, con il responsabile di contratto e il Security IT Manager (se nominato) oppure con il responsabile della sicurezza del committente, i contenuti e i formati dei cataloghi al fine della condivisione e l'aggiornamento di tali informazioni.

Nel caso in cui per le prestazioni affidate dal Titolare al Responsabile, quest'ultimo ritenga di avvalersi di ulteriori soggetti, è obbligato a nominarli quali sub-responsabili del trattamento, assicurandosi che il sub-responsabile presenti garanzie sufficienti in termini di competenza e conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche e organizzative appropriate di modo che il trattamento dei dati risponda ai principi e alle esigenze del GDPR, e deve:

- sottoporre a preventiva autorizzazione scritta e specifica del Titolare qualsiasi affidamento di trattamenti ad ulteriore responsabile(cd. “sub-responsabile”);
- far rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile del trattamento, riportati in uno specifico contratto o atto di nomina. Qualora il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile
- far adottare agli eventuali sub-responsabili, idonee e preventive misure di sicurezza tecniche ed organizzative appropriate, atte ad eliminare o, comunque, a ridurre al minimo qualsiasi violazione, rischio di distruzione o perdita, anche accidentale, dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme, nel rispetto delle disposizioni contenute nell’articolo 32 del GDPR;

I trattamenti affidati dal Responsabile al sub responsabile riguardano: i dati dell'Anagrafe degli studenti universitari e dei laureati, uniti alle Comunicazioni Obbligatorie rilevate dal Sistema Informativo Lavoro (SIL).

Art. 3 - Inadempienze e controversie

Eventuali controversie che dovessero insorgere legate alla possibilità che il Responsabile possa aver agito in modo difforme o contrario alle legittime istruzione del Titolare oppure abbia adottato misure di sicurezza inadeguate rispetto al rischio del trattamento, saranno risolte, in prima istanza, secondo procedimento amichevole tra le Parti tramite richiesta da parte del Titolare di apertura di una procedura di conciliazione della controversia. Un referente del Titolare (il DPO, se nominato) e un referente del Responsabile (il DPO, se nominato) porteranno avanti la composizione della controversia in tempi ragionevoli. Qualora dopo aver esperito ogni tentativo di conciliazione, la controversia non venga risolta entro 30 giorni dall’avvio della procedura, e venga altresì comprovata la causa esclusiva di inadempienza da parte del Responsabile, questi risponderà del danno causato agli “interessati” e il Titolare potrà risolvere la convenzione, salvo il risarcimento del maggior danno.

Firma Titolare*

Ing. Fabio Martelli

Firma Responsabile esterno*

Direttore pro-tempore dell’IRPET- STEFANO CASINI BENVENUTI

Luogo	data
Firenze	20/11/2020

(*) “Documento informatico sottoscritto con firma digitale ai sensi del T.U. 445/2000 e del D.Lgs 82/2005 e rispettive norme collegate, il quale sostituisce il documento cartaceo e la firma autografaL’originale informatico è stato predisposto e conservato presso IRPET in conformità alle regole tecniche di cui all’art. 71 del D.Lgs. 82/2005. Nella copia analogica la sottoscrizione con firma autografa è sostituita dall’indicazione a stampa del nominativo del soggetto responsabile secondo le disposizioni di cui all’art. 3 del D.Lgs. n. 39/1993