



REGIONE DEL VENETO

Azienda Regionale per il Diritto allo Studio Universitario

Copia conforme all'originale

DECRETO DEL COMMISSARIO STRAORDINARIO

N. 26 DEL 06 NOVEMBRE 2018

**OGGETTO: REGOLAMENTO UE 2016/679 PER LA PROTEZIONE DEI DATI PERSONALI.
ADOZIONE DELLE MISURE ORGANIZZATIVE, DOCUMENTALI E TECNICHE.**

RELAZIONE

PREMESSO che l'attività di trattamento dei dati personali è disciplinata dal "Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, di seguito GDPR ("General Data Protection Regulation") relativo alla protezione delle persone fisiche con riguardo al trattamento dei Dati personali, nonché alla libera circolazione di tali Dati, che abroga la direttiva 95/46/CE.

ATTESO che il GDPR si propone di armonizzare le previsioni in materia di privacy a livello europeo, abrogando la Direttiva 95/46/CE, recepita nel nostro ordinamento dal Decreto Legislativo n.196/2003 (Codice della Privacy).

CONSIDERATO che con Decreto Legislativo n. 101 del 10.08.2018 recante "*disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016*" è stata introdotta nell'ordinamento italiano la normativa di coordinamento, finalizzata ad armonizzare le norme enunciate nel Codice della Privacy con quelle introdotte dal GDPR, entrato in vigore il 25 maggio 2016, applicabile obbligatoriamente in tutti i suoi elementi e direttamente in ciascuno degli Stati membri a decorrere dal 25 maggio 2018;

ATTESO che

- nel nuovo assetto normativo, il Titolare del trattamento (*data controller*) è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*" (art. 4. par. 1, n. 7 GDPR);
- per effetto del GDPR il Titolare del Trattamento è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa, sia nazionale che internazionale, in materia di protezione dei dati personali;

- il GDPR innova profondamente la materia della privacy, introducendo il principio di “responsabilizzazione” (*accountability*) in virtù del quale è affidato al Titolare del trattamento il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto dei principi e delle disposizioni del GDPR, adottando le misure più opportune e comprovando il conseguimento degli obiettivi raggiunti nel rispetto dei principi che presidono il trattamento (lecito) dei dati personali;
- l’implementazione del “sistema privacy” delineato dal GDPR implica la necessità di generare nell’organizzazione la piena consapevolezza dei rischi inerenti ai trattamenti dei dati e le responsabilità connesse, nonché l’affermazione di una cultura della protezione dei dati quale parte integrante dell’intero asset informativo di un’organizzazione, sotto il profilo dei diritti e delle libertà fondamentali dell’individuo;

POSTO che l’A.R.D.S.U. – ESU di Venezia, nella sua veste di Titolare del trattamento, già all’indomani dell’entrata in vigore del GDPR, ha posto in essere alcune azioni di carattere organizzativo, gestionale e documentale volte ad ottemperare agli obblighi del Regolamento UE n. 2016/679, fra le quali si segnala:

- Individuazione del ruolo e designazione del “Data Protection Officer” (DPO), previsto dall’art.37 del GDPR. Con decreto del Direttore Generale n.128 del 22 maggio 2018, attesa la mancanza all’interno dell’organizzazione di personale idoneo a ricoprire il ruolo, si provvedeva ad affidare, a seguito trattativa diretta sul MePA, il predetto servizio di Responsabile della Protezione dei Dati (RPD), designando l’avv. Francesca Gravili dello Studio Associato Servizi Professionali Integrati (FIELD FISHER-S.A.S.P.I.);
- Adozione delle prime disposizioni per la protezione dei dati personali in attuazione del Regolamento UE 679/2016 e istituzione del Registro unico delle attività del titolare del trattamento e delle categorie dei trattamenti, con Decreto del Commissario Straordinario n. 11 del 23 maggio 2018 ad oggetto: Disposizioni per la protezione dei dati personali in attuazione del regolamento UE 2016/679 “Regolamento generale per la protezione dei dati”.

DATO ATTO che, a seguito dell’avvenuta nomina del DPO, è stato attivato un *gruppo di lavoro GDPR*, da intendersi quale gruppo di lavoro multidisciplinare, anche a supporto delle attività del DPO, al fine di dare attuazione alle disposizioni del GDPR cui è stato affidato il compito di supportare il Titolare del Trattamento nella definizione delle misure da adottarsi per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di privacy.

CONSIDERATO che l’Ente, che svolge attività volta a garantire e promuovere il Diritto allo Studio Universitario, nell’ambito delle competenze affidate all’ESU dalla Regione Veneto (Legge Regionale n. 8 del 7 aprile 1998), fornendo assistenza e sostegno agli studenti universitari mediante l’erogazione di benefici e servizi, tra cui l’ammissione alle residenze e alloggi universitari, l’erogazione di Borse di Studio e prestiti nonché le provvidenze per studenti disabili, sulla base delle risultanze dell’attività di *Risk Assessment* condotte con il supporto del *gruppo di lavoro GDPR*, ha elaborato un *set* di documenti conformi al GDPR (informative, nomine a responsabili, *policies* varie, *etc.*) messi a disposizione dei Destinatari.

ATTESO che nell’ambito delle attività svolte dal gruppo di lavoro GDPR sono stati predisposti e condivisi i seguenti elaborati:

- *Data Protection Master Policy* al fine di fornire il quadro relativo all’attuazione del GDPR all’interno dell’Ente definendo, nell’ottica dell’*accountability*, l’organizzazione *privacy*

dell'Azienda. La *Policy* fornisce, altresì, indicazioni in merito a come viene disciplinato il Trattamento di Dipendenti, Studenti e Ospiti e Fornitori, nonché di altri soggetti eventualmente Interessati, da parte dell'Ente, "disegnato" sulla base del proprio *business*, tramite l'indicazione di regole interne conformi alle disposizioni del GDPR;

- alcuni modelli d'informazione (che corrispondono all'informativa prevista dal Codice Privacy), da fornire al personale, ai terzi interessati partecipanti a gare e contratti, a clienti e stakeholders, ove sono previste tutte le informazioni di cui all'art.13 del *GDPR*, fermo restando che i modelli medesimi sono da considerarsi quali documenti "dinamici" e, pertanto, soggetti a variazioni e/o integrazioni;
- procedura per la gestione di Data Breach e del registro delle violazioni;
- *Subject Access Request – SAR* contenente la disciplina relativa alla procedura di gestione delle richieste pervenute dagli Interessati e dai dipendenti, inerenti all'accesso ai dati e all'esercizio dei diritti ad essi relativi;

CONSIDERATO che il Registro dei trattamenti è stato e sarà implementato da questa Azienda, secondo la propria policy in materia di privacy, la propria organizzazione e i documenti di protezione dati, nonché in relazione agli applicativi software destinati a gestire i singoli trattamenti, fermo restando che il registro medesimo è da considerarsi quale documento "dinamico" e, pertanto, soggetto a variazioni e/o integrazioni. Esso è depositato presso l'Ufficio Servizi Informatici – IT, a disposizione sia dell'Autorità Garante per la Protezione dei Dati Personali (Garante Privacy), sia di chiunque possa vantare un legittimo interesse alla sua consultazione;

ACQUISITA la documentazione elaborata dal gruppo di lavoro, il *Data Protection Master Policy* che fornisce il quadro relativo all'attuazione del GDPR all'interno dell'Ente definendo, nell'ottica dell'*accountability*, l'organizzazione *privacy* dell'Azienda e la *Subject Access Request – SAR* contenente la disciplina relativa alla procedura di gestione delle richieste pervenute dagli Interessati e dai dipendenti, inerenti all'accesso ai dati e all'esercizio dei diritti ad essi relativi;

ATTESO inoltre che il medesimo gruppo di lavoro ha altresì redatto una prima procedura relativa ai *data breach* ex art. 32 del *GDPR*, a disposizione dell'Autorità Garante per la Protezione dei Dati Personali (Garante Privacy), in cui sono state previste le modalità operative in ordine alla procedura di gestione del *data breach* interno/esterno alla struttura.

EVIDENZIATO inoltre come il vigente sistema normativo preveda che il Titolare del trattamento possa affidare a figure interne all'organizzazione specifici compiti e funzioni connessi al trattamento di dati personali, espressamente designate, che operano sotto la propria autorità e responsabilità, ora denominati "*Referenti Privacy*", e che lo stesso Titolare, o i suoi delegati, possano individuare le "*persone autorizzate al trattamento dei dati*".

RITENUTO di procedere all'individuazione e alla nomina dei "*Referenti Privacy*" e delle "*persone autorizzate*" in coerenza con l'assetto organizzativo dell'Azienda in ordine ai diversi profili di responsabilità, come di seguito indicato:

- "*Referenti Privacy HR*", figura individuata nel ruolo del Direttore Generale e del Dirigente;
- "*Referenti Privacy Generale*", figura individuata nel ruolo del titolare di Posizione Organizzativa;

- “*Persone autorizzate al trattamento*”, tutti gli altri dipendenti e collaboratori, a qualsiasi titolo, dell’Azienda che nell’esercizio delle proprie funzioni svolgano attività di trattamento dei dati personali, nel rispetto delle relative istruzioni.

CONSIDERATO che:

- il GDPR dispone altresì, all’art.28, che qualora il trattamento dei dati debba essere effettuato da soggetto esterno all’organizzazione del Titolare, questi debba incaricare tale soggetto quale “Responsabile del trattamento”, previa contrattualizzazione mediante contratto o altro atto giuridico a norma del diritto dell’UE o degli Stati membri e solo qualora presenti “garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell’interessato”;
- il contratto, che vincola il Responsabile al Titolare, deve definire la durata del trattamento, la natura e le finalità del medesimo, le tipologie dei dati trattati e le categorie di interessati, gli obblighi e i diritti del Titolare, a patto che il Responsabile sia autorizzato a trattare i dati solo previa istruzione documentata del Titolare e offra tutte le garanzie previste dal succitato art.28;
- il nuovo impianto normativo lambisce pertanto anche il ruolo del Responsabile del trattamento, il quale è insignito di nuovi compiti rispetto al passato, condivide in certa misura le responsabilità del Titolare in ordine al risarcimento del danno a terzi, ed è oggetto di autonome sanzioni amministrative, a differenza di quanto avveniva con il Codice Privacy, ove la sanzione amministrativa era sempre diretta contro il Titolare;
- l’individuazione del Responsabile non avviene più, quindi, a discrezione del Titolare, ma è un atto dovuto e in ogni caso la designazione del Responsabile emerge “ex se” dallo stato di fatto. Il Titolare e il Responsabile regolano, come visto, i loro rapporti contrattualmente, ma non sarà possibile forzare l’assetto contrattuale per definire i reciproci ruoli: l’assetto contrattuale rispecchierà, invece, il concreto “potere” che questi soggetti eserciteranno sul trattamento dei dati personali, prendendo o meno decisioni in ordine alle finalità e ai mezzi del trattamento stesso.

RITENUTO, nelle more dell’emanazione, da parte del Garante Privacy, di un modello di contratto da adottare da parte di ciascun Titolare per il conferimento dell’incarico di Responsabile del trattamento, da intendersi quale Responsabile esterno all’organizzazione aziendale, di predisporre un modello di contratto per la nomina a Responsabile esterno di tutti quei soggetti giuridici (enti, società, associazioni, ecc.) che trattano dati sensibili per conto di questa Azienda nell’ambito di rapporti contrattuali in essere o di contratti/convenzioni che verranno stipulati, fermo restando che il modello medesimo dovrà essere adattato alle diverse tipologie di contratto, secondo le specificità delle singole attività affidate in outsourcing.

RAVVISATA inoltre l’opportunità di fornire al personale indicazioni in merito alle modalità di funzionamento degli strumenti aziendali loro assegnati o da essi comunque utilizzati e le regole di comportamento da rispettare per un corretto utilizzo dei predetti strumenti aziendali anche al fine di ridurre rischi e/o minacce alla sicurezza dei sistemi e/o dei dati in essi contenuti, con particolare riguardo ai dati personali e/o al patrimonio immateriale dell’Azienda.

IL COMMISSARIO STRAORDINARIO

PRESO ATTO di quanto espresso in premessa;

VISTO il Regolamento UE 679/2016 “regolamento sulla protezione dei dati”;

VISTO il D.Lgs. n. 101 del 10.08.2018 recante "*disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016*" che adegua la normativa italiana al nuovo Regolamento Ue 2016/679 sulla privacy;

VISTA la Legge Regionale 7 aprile 1998 n. 8;

DECRETA

1. Di approvare le premesse del presente atto come sopra esposte, che conseguentemente devono ritenersi parte integrante e sostanziale del presente dispositivo;
2. di adottare il Registro delle attività di trattamento, implementato da questa Azienda sulla base delle proprie specificità e depositato presso l'Ufficio Servizi Informatici – IT a disposizione sia dell'Autorità Garante per la Protezione dei Dati Personali, sia di chiunque possa vantare un legittimo interesse alla sua consultazione;
3. di adottare il Data Protection Master Policy che fornisce il quadro relativo all'attuazione del GDPR all'interno dell'Ente definendo, nell'ottica dell'*accountability*, l'organizzazione *privacy* dell'Azienda e la Subject Access Request – SAR contenente la disciplina relativa alla procedura di gestione delle richieste pervenute dagli Interessati e dai dipendenti, inerenti all'accesso ai dati e all'esercizio dei diritti ad essi relativi;
4. di adottare i modelli d'informazione, ai sensi dell'art.12 del *GDPR*, a disposizione dell'Autorità Garante per la Protezione dei Dati Personali, fermo restando che il modello medesimo è da considerarsi quale documento “dinamico” e, pertanto, soggetto a variazioni e/o integrazioni;
5. di approvare la procedura relativa ai data breach depositata presso l'Ufficio Servizi Informatici – IT a disposizione dell'Autorità Garante per la Protezione dei Dati Personali (Garante Privacy);
6. di individuare i soggetti “Referenti Privacy HR” nelle persone del Direttore Generale e del Dirigente pro-tempore, i soggetti “Referenti Privacy Generale” nelle persone dei titolari di Posizione Organizzativa e di stabilire che “persone autorizzate al trattamento” siano da intendersi tutti gli altri dipendenti e collaboratori, a qualsiasi titolo, di questa Azienda, qualora nell'esercizio delle proprie funzioni svolgano attività di trattamento dei dati personali.
7. di adottare il modello di contratto per la nomina a Responsabile esterno di tutti quei soggetti giuridici che trattano dati sensibili per conto di questa Azienda nell'ambito di rapporti contrattuali in essere o di contratti/convenzioni che verranno stipulati, fermo

restando che il modello medesimo dovrà essere adattato alle diverse tipologie di contratto, secondo le specificità delle singole attività affidate in *outsourcing*;

8. di adottare il Regolamento per l'utilizzo degli strumenti aziendali e le istruzioni alle persone autorizzate alle operazioni e alle modalità di Trattamento dei dati personali;
9. di dare atto che il presente atto deliberativo non comporta l'assunzione di alcun onere finanziario in capo a questa Azienda.

Venezia, lì 6 novembre 2018

IL DIRETTORE
Dr. Daniele Lazzarini

IL COMMISSARIO STRAORDINARIO
Dr. Salvatore Castagnetta

UFFICIO PROPONENTE: DIREZIONE

Il Responsabile della struttura proponente, o suo delegato, incaricato dell'esecuzione, che ha istruito ed espletato in ogni sua parte la pratica, ne attesta la conformità agli atti, dichiara l'avvenuta regolare istruttoria, la compatibilità con la vigente legislazione comunitaria, statale e regionale, controfirmando la proposta del presente atto.

Venezia, li 6 novembre 2018

IL DIRETTORE
Daniele Lazzarini

UFFICIO RAGIONERIA

PROVVEDIMENTO REGISTRATO AL N. Progr. /

ai sensi del D. Lgs. 118/2011 - visto ed assunto l'impegno -

di EURO N. Cap. C R

di EURO N. Cap. C R

ai sensi del D. Lgs. 118/2011 - visto ed assunto l'accertamento

di EURO N. Cap. C R

di EURO N. Cap. C R

Nel caso di assunzioni di impegni e/o accertamenti in più di due capitoli

visti e registrati nel bilancio, come indicato nella sezione dispositiva del provvedimento

imputazione contabile già effettuata con DECRETO n.

DECRETO non soggetto ad imputazioni contabili.

Venezia, li _____
Emanuela Di Flavia

IL RESPONSABILE DELL'UFFICIO RAGIONERIA

COPIA CONFORME

Si attesta che la presente copia è conforme all'originale conservato agli atti, e viene rilasciata in carta libera per uso amministrativo.

Venezia, li _____

UFFICIO SEGRETERIA

ATTESTAZIONE DI PUBBLICAZIONE

Il presente Decreto viene pubblicato, anche ai fini della pubblicità degli atti e della trasparenza amministrativa, mediante affissione all'Albo dell'Ente, per quindici giorni interi e consecutivi a decorrere dalla data odierna, come prescritto dalla normativa vigente.

Venezia, li _____

UFFICIO SEGRETERIA