

DETERMINAZIONE N° 178 DEL 21.06.2018

IL DIRETTORE GENERALE: ING. GIANLUCA BASILE

SETTORE: DIREZIONE GENERALE

IL RESPONSABILE DEL PROCEDIMENTO: ING. GIANLUCA BASILE

Oggetto: Adozione del Disciplinare Interno in materia di tutela della privacy

IL DIRETTORE GENERALE

PREMESSO:

Che la Legge regionale 5 aprile 2016, n. 6 *"Prime misure per la razionalizzazione della spesa e il rilancio dell'economia campana – Legge collegata alla legge regionale di stabilità per l'anno 2016"* all'art. 18, comma 1, testualmente recita *"1. La Regione Campania promuove le necessarie azioni per lo svolgimento dell'edizione 2019 delle Universiadi in Campania, in esito alla delibera del comitato esecutivo della Federazione Internazionale dello Sport Universitario (FISU), in data 5 marzo 2016, riconoscendone la valenza di grande evento:*

- a) per la promozione culturale, sportiva, turistica ed economica del territorio regionale, in ambito internazionale;*
- b) per il potenziamento dell'impiantistica sportiva e la diffusione dello sport, in ambito regionale;*
- c) per lo sviluppo delle reti infrastrutturali e di telecomunicazione al servizio dell'evento e d'interesse dei territori interessati;*
- d) per la valorizzazione ed integrazione del sistema universitario campano.*

CONSIDERATO CHE:

- la Legge 27/12/2017, comma 375, n. 205, pubblicata sulla G.U. Serie Generale n. 302 del 29/12/2017 Suppl. Ordinario n. 62, all'art. 1 comma 375, al fine di assicurare la realizzazione dell'Universiade Napoli 2019, prevede che con decreto del Presidente del Consiglio dei ministri, d'intesa con il Presidente della Regione Campania, è nominato un Commissario straordinario *"il quale opera in via esclusiva con il compito di provvedere all'attuazione del piano di interventi volti alla progettazione e realizzazione dei lavori e all'acquisizione di servizi e beni, anche per eventi strettamente connessi allo svolgimento della manifestazione sportiva...omissis..."*;
- ai sensi della su citata legge (art. 1, comma 376) il Commissario Straordinario *"...subentra ai soggetti istituiti ivi compresa l'Agenda Regionale Universiadi 2019, che può previa intesa svolgere attività di supporto tecnico, per definire, coordinare e realizzare le attività necessari per l'Universiade 2019"*;
- con D.P.C.M. del 5/02/2018, registrato alla Corte dei Conti in data 23/02/2018 Reg.ne- Prev. n. 360, notificato l'8 marzo 2018, è stato nominato Commissario straordinario per la realizzazione dell'Universiade Napoli 2019 il Prefetto dr.ssa Luisa Latella;
- con D.G.R. Campania n. 69 del 13/02/2018 recante *"Summer Universiade Napoli 2019 – Adempimenti di cui all'art. 1, commi 375 e ss. Della L. n. 205/2017 – Modifiche Statutarie"* si è provveduto alle modifiche dello Statuto dell'ARU che a far data dalla sottoscrizione di apposita convenzione, svolge un ruolo di struttura tecnica a supporto del Commissario straordinario D.P.C.M. del 5/02/2018;
- in data 26/03/2018 è stato sottoscritto l'Accordo di collaborazione ai sensi dell'art. 1, comma 376, della Legge 27 dicembre 2017 n. 205 tra il Commissario straordinario per l'Universiade Napoli 2019 e l'ARU 2019 per lo svolgimento di supporto tecnico al Commissario

Straordinario;

- l'intervento di cui trattasi, ai sensi dell'art.5 del predetto Accordo di Collaborazione è inserito nella programmazione generale della manifestazione ed è a titolarità ARU.

RILEVATO CHE

- in data 25 maggio 2018 è entrato in vigore il Regolamento (UE) 2016/679 in materia di privacy che prevede nuovi obblighi per la protezione dei dati personali, una nuova figura professionale e un nuovo e severissimo trattamento sanzionatorio;
- il nuovo quadro normativo impone di gestire una serie di "informazioni" che possono essere considerate, ai sensi del D.Lgs. 196/2003 e s.m.i., "dati personali" quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che l'ente adotti una serie di misure minime ed idonee previste dalle norme;
- altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "informazioni riservate", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l'agenzia è chiamata a garantire la riservatezza;
- con determina n. 153 del 21.05.2018 è stato nominato il Responsabile della protezione dei dati personali – dott.ssa Annapaola Voto, Dirigente dell'Area Istituzionale;
- il Responsabile della protezione dei dati personali in ottemperanza a quanto richiesto dalla nuova normativa sulla tutela della privacy ha chiesto l'autorizzazione al Direttore Generale a redigere un disciplinare interno in materia di tutela della privacy, a cui tutti i dipendenti dell'Agenzia sono tenuti all'osservanza;

VISTI

- Lo Statuto dell'Agenzia Regionale Universiadi 2019;
- Il regolamento sull'ordinamento degli uffici e servizi;
- il D.lgs. 50/2016
- la legge sulla privacy;
- la determina n. 153 del 21.05.2018;

DETERMINA

Per le motivazioni di cui in premessa che qui si intendono per riportate e trascritte di

- **di adottare** il Disciplinare Interno in materia di tutela della privacy redatto ai sensi dei provvedimenti del Garante della Privacy (deliberazione n. 13 del 01/03/2007 – pubblicata sulla GU n. 58 del 10 marzo 2007);
- **di trasmettere** la presente determinazione a tutti i Dirigenti e dipendenti dell’Agenzia Regionale Universiadi – ARU 2019, comunicando l’obbligo di osservanza del disciplinare interno in materia di tutela della privacy;
- **di dare atto** che ai sensi dell’articolo 29 del D.Lgs. 50/2016 tutti gli atti relativi alla procedura in oggetto saranno pubblicati e aggiornati sul profilo del committente, nella sezione “Amministrazione Trasparente”, con l’applicazione delle disposizioni di cui al decreto legislativo 14 marzo 2013, n. 33.

IL DIRETTORE GENERALE
Ing. Gianluca Basile





REGOLARITÀ CONTABILE

SI APPONE, ai sensi dell'art. 36 e seguenti del D.lgs. 118/2011 così come modificato dal D.Lgs. 10 agosto 2014, 126 il visto di regolarità contabile con attestazione della copertura finanziaria.

NON SI APPONE ai sensi dell'art. 36 e seguenti del D.lgs. 118/2011 così come modificato dal D.Lgs. 10 agosto 2014, 126 il visto di regolarità contabile con attestazione della copertura finanziaria per la motivazione indicata con nota prot. _____ del _____, che si allega.

IMPEGNO DI SPESA

Capitolo Bilancio di previsione 2018/2020 N.

Impegno n° _____ Importo €. _____

Napoli, lì _____

IL RESPONSABILE DEL SETTORE FINANZIARIO

Ing. Gianluca Basile

CERTIFICAZIONE DI PUBBLICAZIONE

Si certifica che copia conforme all'originale della presente determinazione è stata pubblicata sul sito dell'Agenzia Regionale Universiadi in data _____

Lì, _____

IL RESPONSABILE DELLA TRASPARENZA

COPIA CONFORME

Si certifica che la presente è copia conforme all'originale.

Lì, _____

TRASPARENZA

IL RESPONSABILE DELLA



DISCIPLINARE INTERNO IN MATERIA DI TUTELA DELLA PRIVACY

Regole di condotta ed obblighi dei collaboratori in relazione all'uso degli strumenti informatici, di internet e della Posta Elettronica redatto anche ai sensi del provvedimento del Garante della Privacy (Deliberazione n. 13 del 01/03/2007 – pubblicata sulla GU n. 58 del 10 marzo 2007) comprensivo di alcune note per la gestione dei dati cartacei

ART. 1 – DEFINIZIONI DI RIFERIMENTO

- a)** "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- b)** "dato personale", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- c)** "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;
- d)** "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- e)** "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- f)** "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- g)** "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- h)** "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- i)** "interessato", la persona fisica cui si riferiscono i dati personali;
- l)** "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- m)** "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

- n) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- o) "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- p) "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti

ART. 2 – GESTIONE PASSWORD

Le password possono essere un metodo di autenticazione assegnato dall'agenzia per garantire l'accesso protetto ad uno strumento hardware oppure ad un applicativo software. La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e dell'agenzia nel suo complesso. Nel tempo anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza. Altra buona norma è quella di non memorizzare la password su supporti facilmente intercettabili da altre persone.

L'Incaricato, da parte sua, per una corretta e sicura gestione delle proprie password deve rispettare le regole seguenti:

1. Le password sono assolutamente personali e non vanno mai comunicate ad altri;
2. Occorre cambiare immediatamente una password non appena si abbia alcun dubbio che sia diventata poco "sicura";
3. Le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali e numeri;
4. Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
5. Le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password.
6. Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'agenzia.

In alcuni casi, sono implementati meccanismi che consentono all'Incaricato fino ad un numero limitato di tentativi errati di inserimento della password oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account e l'intero sistema viene bloccato per alcuni minuti.

NB: La password ideale deve essere complessa, senza alcun riferimento, ma facile da ricordare.

ART. 3 – L'UTILIZZO DELLA POSTA ELETTRONICA "UNIVERSIADE"

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa. L'uso per motivi personali deve essere moderato ed è tollerato esclusivamente ai sensi dell'articolo seguente. Gli Incaricati possono avere in utilizzo indirizzi nominativi di posta elettronica. Le caselle e-mail possono meglio

essere assegnate con natura impersonale (tipo info, amministrazione, fornitori, direttore, direttore sanitario, consulenza, ...) proprio per evitare ulteriormente che il destinatario delle mail possa considerare l'indirizzo assegnato al dipendente "privato", ai sensi dei suggerimenti del Garante a tal proposito. Gli Incaricati assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. L'organizzazione è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte degli Incaricati e allo scopo prevede le seguenti misure:

1. In caso di ricezione sulla e-mail aziendale di posta personale si avverte di cancellare immediatamente ogni messaggio al fine di evitare ogni eventuale e possibile back up dei dati.
2. Avvisare l'organizzazione quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta.
3. È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio dell'agenzia per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'organizzazione, nonché utilizzare il dominio dell'organizzazione per scopi personali.
4. È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale.
5. È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.
6. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'agenzia informazioni riservate o comunque documenti di lavoro, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.
7. È vietato utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni. Nella maggior parte dei casi sarà il sistema stesso a limitare la dimensione degli allegati che è possibile inviare (nel caso della posta elettronica "universiade" la dimensione massima consentita dal sistema è 10 MB).

ART. 4 – RISERVATEZZA DEI DATI CARTACEI: "CLEAR DESK POLICY"

Gli Incaricati sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Gli Incaricati sono invitati dall'organizzazione ad adottare una "politica della scrivania pulita". Ovvero si richiede agli incaricati di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dell'ente.

I principali benefici di una politica della scrivania pulita sono:

- 1) Una buona impressione a clienti e fornitori che visitano la nostra agenzia;
- 2) La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;
- 3) La riduzione che documenti confidenziali possano essere sottratti all'agenzia.

In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi

contenuti. Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura degli Incaricati riporre in luogo sicuro (armadio, cassettera, archivio, ...) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti nell'agenzia. A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra. Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica. Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archivarli digitalmente. E' necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.

ART. 5 – PUBBLICAZIONE ATTI NELLA SEZIONE “AMMINISTRAZIONE TRASPARENTE”

Come è noto, l'agenzia è tenuta alla pubblicazione degli atti in ottemperanza al Decreto legislativo 14 marzo 2013, n. 33 “Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni”, che ha riordinato e semplificato la normativa in materia di obblighi di pubblicità, trasparenza e diffusione delle informazioni da parte delle amministrazioni pubbliche ai sensi dell'art. 1 c. 35 della legge n. 190/2012 “Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione”.

Il Responsabile della prevenzione della corruzione e della trasparenza è tenuto agli adempimenti delle succitate leggi e a garantire che, all'atto della pubblicazione, che dagli atti vengano espunti dati personali, identificativi e sensibili, ed ogni altro riferimento atto a rivelare informazioni tutelate dalle leggi sulla privacy. Con determina dirigenziale n. 1 del 9 gennaio 2017 è stato nominato il Responsabile della prevenzione della corruzione e della trasparenza dell'ARU 2019-

Qualora l'agenzia abbia mancato di adempiere ai propri obblighi di pubblicità e trasparenza degli atti, è possibile ricorrere all'istituto dell'accesso civico ex art. 5 del decreto legislativo 14 marzo 2013, n. 33 (“decreto trasparenza”) e al comma 1, che riconosce a chiunque il diritto di richiedere i documenti, le informazioni o i dati che le pubbliche amministrazioni abbiano omesso di pubblicare in rete pur avendone l'obbligo. Con lo strumento dell'accesso civico chiunque può quindi vigilare, attraverso il sito web istituzionale dell'ARU 2019, sul corretto adempimento formale degli obblighi di pubblicazione da parte dell'Amministrazione. Va altresì ricordato che è stato introdotto all'art. 5, comma 2, un nuovo diritto generalizzato, inserito nella sezione “accesso civico” dell'amministrazione trasparente e che consente a chiunque di accedere ai dati e documenti detenuti dalle pubbliche amministrazioni, ulteriori a quelli sottoposti ad obbligo di pubblicazione, con il limite del rispetto degli interessi pubblici e privati giuridicamente rilevanti e specificati nel nuovo art. 5-bis (esclusioni e limiti).

IL RESPONSABILE DELLA TUTELA DELLA PRIVACY

Dott.ssa Annapaola Voto

