NOMINA DI PERSONA AUTORIZZATA AL TRATTAMENTO DEI DATI PERSONALI E REFERENTE PRIVACY ED ISTRUZIONI OPERATIVE PER IL TRATTAMENTO

Opera Universitaria di Trento, in qualità di Titolare del trattamento dei dati personali, con sede in Trento, via della Malpensada n. 82/A,

PREMESSO CHE

- Opera Universitaria di Trento, ai sensi dell'art 28 Codice Privacy e dell'articolo 24 del Regolamento UE n. 2016/679, è Titolare dei trattamenti di dati personali;
- l'art 30 del Codice privacy definisce espressamente l'incaricato del trattamento;
- l'art. 4 n. 10 del Regolamento UE n. 2016/679 in materia di protezione dei dati personali prevede che la persona autorizzata al trattamento dei dati personali sia sotto l'autorità diretta del titolare o responsabile del trattamento;

Tutto ciò premesso Opera Universitaria di Trento,

NOMINA

il dott. Paolo Fontana, quale **Referente Privacy** interno.
Il referente privacy si avvale altresì della collaborazione del sig. Fabio Daprà.
Occorre precisare che Ella, in qualità di Referente Privacy, in caso di violazione dei dati personali, è un componente permanente del Team Crisi unitamente al Responsabile IT ed al DPO.

A) RESPONSABILITÀ GENERALI

Le Responsabilità del Referente Privacy, alle dipendenze gerarchiche del Titolare sono le seguenti:

a) del controllo del rispetto delle istruzioni in materia di trattamento di dati personali a carico dei propri collaboratori
b) aggiornare le informative verso gli interessati;
c) supportare le funzioni dell'Ente nelle nomine verso autorizzati, Responsabili esterni del trattamento, altre funzioni;
d) supportare l'Amministratore di sistema nell'applicazione del provvedimento a suo carico;
e) supportare le funzioni dell'Ente nell'applicazione di specifici provvedimenti emessi dal Garante;
f) essere membro del Team crisi che gestisce eventuali situazioni di Data Breach
g) partecipare a riunioni ogni qualvolta si introduca all'interno dell'Ente una nuova tecnologia o debbano essere attuate campagne o operazioni che riguardino il trattamento dei dati personali e impostare unitamente al Titolare del trattamento la valutazione preventiva di impatto del rischio;
h) partecipare a riunioni ogni qualvolta si introducano nuove misure sulla sicurezza o potenziali sistemi di controllo a distanza dei dipendenti o qualora si vogliano applicare politiche dell'ente che impattano sulla riservatezza dei dipendenti;
i) conservare l'archivio della documentazione richiesta dal GDPR;
j) mettere in atto le disposizioni richieste dal DPO in materia di protezione dei dati; relazionare sullo stato di avanzamento ed eventuali problematiche;
a) supportare il DPO nel predisporre e tenere sotto controllo il piano delle attività previste;
b) supportare il DPO nel pianificare e condurre o sorvegliare la conduzione di attività di audit (sia di conformità al GDPR che relativi all'applicazione delle procedure interne che impattano sul GDPR); tenere sotto controllo lo stato di avanzamento delle eventuali criticità emerse nel corso dell'audit;
c) supportare il DPO nel tenere sotto controllo lo stato di avanzamento delle misure pianificate per la mitigazione dei rischi;

B) OBBLIGHI DEL REFERENTE PRIVACY

Il Referente Privacy ha l'obbligo di partecipare alle iniziative formative in materia di trattamento dei dati proposte dal Titolare del trattamento ai sensi dell'art 29 del Reg. UE 2016/679.

C) PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI

ai sensi dell'art. 11 del Codice Privacy e dell'art 5 del Regolamento UE 2016/679

Nello svolgimento del trattamento devono essere osservate le norme di legge e di regolamento in materia di protezione dei dati personali ed in particolare:

- ✓ i dati devono essere trattati in modo **lecito, corretto e trasparente** nei confronti degli interessati **esatti** e se necessario **aggiornati**;
- ✓ il trattamento dei dati deve rispettare il principio **di pertinenza e non eccedenza** rispetto alle finalità del medesimo;
- ✓ l'accesso ai soli dati personali la cui conoscenza sia strettamente indispensabile per adempiere ai compiti affidati.

D) ISTRUZIONI OPERATIVE

D1) ISTRUZIONI GENERALI

Il referente nello svolgimento delle proprie mansioni è tenuta a:

- **verificare** che ciascuna operazione di comunicazione e diffusione dei dati sia conforme alle disposizioni di legge e regolamento, adempimento di un contratto, soddisfacimento della richiesta dell'interessato;
- **collaborare**, con le altre persone autorizzate al trattamento del medesimo trattamento, esclusivamente per i fini dello stesso e nel rispetto delle indicazioni fornite;
- **non trasmettere**, a soggetti terzi, informazioni circa dati personali trattati. La comunicazione è ammessa soltanto se funzionale allo svolgimento dei compiti affidati, previa autorizzazione del Titolare del trattamento o suo delegato;
- **non creare** nuove ed autonome banche dati senza il permesso del Titolare del trattamento;
- **non trasmettere** dati in qualsiasi forma all'esterno, salvo autorizzazione dal Titolare del trattamento;
- **accertarsi** dell'identità del diretto interessato, prima di fornire informazioni circa i dati personali o il trattamento effettuato;
- **non fornire** dati o informazioni per telefono o per e-mail, qualora non si abbia certezza assoluta sull'identità del destinatario e che tale destinatario sia autorizzato;
- **riporre in un luogo ad accesso controllato,** al termine del periodo di trattamento, i supporti o i documenti cartacei, ancorché non definitivi, contenenti i dati personali;

- **conservare i dati** trattati secondo quanto indicato (tempo/criterio) nel registro dei trattamenti e comunque per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono raccolti e successivamente trattati come da policy privacy dell'Ente.
- **evitare di allontanarsi** dalla scrivania in presenza di ospiti o riporre i documenti e bloccare il pc;
- **a fine turno chiudere** con le apposite chiavi date in dotazione gli archivi di cui fa uso/locali per assicurare la riservatezza dei dati ivi contenuti;
- **segnalare** qualsiasi anomalia e stranezza al Titolare del trattamento/Referente Privacy/DPO/Diretto Responsabile;
- **rispettate** eventuali ulteriori istruzioni, oltre a quelle del presente documento, impartite dal Titolare, nonché le ulteriori istruzioni e direttive impartite da un delegato del Titolare del trattamento/ Referente privacy/DPO/Diretto Responsabile. Tali istruzioni possono assumere la forma di documenti, altri regolamenti, ordini di servizio, ecc.

IN CASO DI DATA BREACH

Anche solo in caso di sospetto di una violazione dei dati:

- il Referente privacy raccoglie le segnalazioni di possibile data breach provenienti dall'interno dell'Ente o dall'esterno di esso in qualsiasi forma;
- il Referente privacy consulta regolarmente il sito del Garante e gli organi di stampa specializzata per verificare eventuali situazioni di potenziale rischio che potrebbero riguardare anche l'attività di Opera Universitaria di Trento.
- In entrambi i casi il Referente privacy comunica via mail con gli altri membri del Team crisi utilizzando la loro casella di posta (al fine di lasciare una traccia) e procedere quindi alla comunicazione telefonica.

Tutte le comunicazioni che provengono da fonte interna o da soggetti esterni devono riportare l'ora.

D2) SUI TRATTAMENTI CON STRUMENTI ELETTRONICI
(ISTRUZIONI UGUALI A TUTTE LE PERSONE AUTORIZZATE)

Per quanto riguarda, in particolare, le elaborazioni e le altre fasi dei trattamenti effettuate attraverso strumenti informatici, Lei disporrà di una o più parole chiave per l'accesso ai dati (password) e di un codice identificativo personale.
Avrà pertanto cura di:

- non rivelare o far digitare la password al personale di assistenza tecnica a colleghi, a esterni;
- non rivelare le password al telefono nè inviarle via fax o e-mail o tramite cellulare; nessuno è autorizzato a chiederle;
- non condividere o cedere a terzi il proprio codice identificativo personale con altri utenti, salvo i casi espressamente previsti;
- la password dovrà essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Essa non dovrà contenere riferimenti a Lei agevolmente riconducibili e dovrà essere modificata almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
- **utilizzare** i mezzi informatici, inclusa la posta elettronica (fornita da Opera Universitaria di Trento) e Internet, esclusivamente per scopi dell'Ente, come previsto nella policy interna sull'utilizzo degli strumenti informatici;

- **non utilizzare** per fini personali, a meno che ciò non sia permesso dal Titolare del trattamento o in caso di emergenza, la propria posta elettronica (questo vale sia per web-mail che per caselle POP configurate su Outlook);
- **non effettuare** download di file o software, senza previa autorizzazione;
- **non accedere** a dati il cui contenuto sia dubbio o illecito né trasferirli nella rete del Titolare;
- **impiegare** sui PC solo software provvisti di licenza, acquistati dal Titolare;
- **salvare** i dati ed i file allegati ai messaggi di posta elettronica, negli archivi dell'Ente, secondo i criteri di archiviazione definiti;
- **non accedere** a servizi non consentiti (es: dropbox, Jumbo mail); nel caso in cui fosse necessario per la propria attività di usufruire di tali servizi confrontarsi con il Titolare del trattamento/Referente Privacy interno/DPO/Diretto Responsabile;
- **non caricare** ed eseguire software di rete o di comunicazione, senza previa verifica dello stesso da parte dell'Amministratore di sistema;
- **non collegare** dispositivi che consentano un accesso, non controllabile, ad apparati della rete di Opera Universitaria di Trento;
- **verificare** l'aggiornamento periodico del proprio software antivirus è vietato scaricare autonomamente software antivirus;
- **custodire** in luogo sicuro i dispositivi rimovibili (es. chiavette usb) contenenti dati personali. Prima di rottamare un qualsiasi dispositivo informatico (compresi i supporti rimovibili) l'incaricato o la persona designata deve cancellare eventuali dati personali contenuti nel dispositivo;
- **non inviare e salvare** dei messaggi che sono discriminanti od offensivi per gruppi religiosi, etnici, appartenenze ai sindacati, orientamento politico, sesso, preferenze sessuali e l'equiparazione dei diritti d'uomini e donne, stato di salute o disabilità. La direzione si riserva la facoltà di verificarne il corretto uso);
- **procedere alla cancellazione** dei supporti magnetici od ottici contenenti dati personali, prima che i medesimi siano riutilizzati. Se ciò non è possibile, essi devono esser distrutti;
- **la cancellazione dei dati** contenuti nelle banche dati elettroniche deve avvenire secondo i tempi/criteri contenuti nel "Registro dei Trattamenti" e previa autorizzazione de Titolare del trattamento o secondo le procedure definite. Potrà essere richieste la verbalizzazione di tale atto. Nel caso di difficoltà nel compiere tali azioni dovrà essere richiesta la collaborazione dell'Amministratore di sistema o di altro soggetto autorizzato;
- **attenersi** ad ulteriori misure di sicurezza, indicate dal Titolare del trattamento o da un suo delegato, nel caso in cui utilizzi dispositivi propri.
- **il furto, il danneggiamento o la perdita, anche accidentale dei dati o l'accesso abusivo agli strumenti a disposizione** (anche personali) contenti dati dell'Ente deve essere comunicato immediatamente al Titolare del trattamento in modo che possa attivare le procedure di data breach.

Inoltre, specificatamente riguardo la *navigazione internet* è vietato:

- navigare su pagine internet che non riguardano l'ambito di lavoro e lasciano intendere le opinioni politiche, religiose o sindacali del collaboratore;
- effettuare operazioni finanziarie (Remote banking, acquisto on-line ecc.) se non hanno attinenza con l'ambito lavorativo e senza autorizzazione esplicita;
- il download di Freeware o Shareware senza autorizzazione esplicita dai dirigenti;
- la registrazione sulle pagine internet non concernente la sfera di competenza;
- la partecipazione a forum, chat, concorsi elettronici non concernenti l'ambito di lavoro e le iscrizioni nei Guest books (anche con pseudonimo).

D3) BANCHE DATI

La visione dei dati, contenuti nelle banche dati, esclude comunque qualsiasi forma di comunicazione, diffusione e trattamento degli stessi che non sia strettamente funzionale all'espletamento dei compiti e che non si svolga nei limiti stabiliti da leggi e regolamenti

D4) SUI TRATTAMENTI SENZA STRUMENTI ELETTRONICI

Per quanto riguarda l'eventuale documentazione cartacea, compresi i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali, gli atti e i documenti contenenti i dati devono essere conservati, dalle persone autorizzare al trattamento dei dati personali, per la durata del trattamento e successivamente riposti in archivi ad accesso controllato, al fine di escludere l'accesso, agli stessi, da parte di persone non incaricate al trattamento.

Nel caso di trattamento di dati sensibili, di dati di minori o di dati giudiziari, gli atti e i documenti, contenenti i dati affidati alle persone autorizzate al trattamento, devono essere conservati in contenitori muniti di serratura, al fine di escludere l'acquisizione degli stessi da parte di persone non autorizzate del trattamento.
La cancellazione dei dati contenuti negli archivi cartacei deve avvenire secondo i tempi/criteri contenuti nel "Registro dei Trattamenti" e previa autorizzazione de Titolare del trattamento. Potrà essere richiesta la verbalizzazione di tale atto. Laddove si renda necessario distruggere i documenti contenenti dati personali, utilizzare gli appositi apparecchi "distruggi documenti"; in assenza di tali strumenti, i documenti dovranno essere triturati in modo da non essere più ricomponibili.
Le persone autorizzate al trattamento sono tenute a segnalare le eventuali necessità di dotazioni e arredi, in modo da poter adempiere a quanto prescritto.

D5) SUI TRATTAMENTI CONCERNENTI CATEGORIE PARTICORI DI DATI PERSONALI ("DATI SENSIBILI") E RELATIVE A CONDANNE PENALI E REATI

Si riportano alcune specifiche misure da applicarsi, oltre a quelle sopra elencate, in caso di trattamento dei dati sensibili, di minori e giudiziari:

- **evitare di inviare**, per fax e e-mail, documenti in chiaro contenenti dati sensibili, di minori o giudiziali: si suggerisce, in tal caso, di inviare la documentazione, senza alcun esplicito riferimento all'interessato (ad esempio, contrassegnando i documenti semplicemente con un codice);
- i documenti, ancorchè non definitivi, ed i supporti recanti dati sensibili, di minori o giudiziari, devono essere conservati, anche in corso di trattamento, in elementi di arredo muniti di serratura e non devono essere lasciati incustoditi in assenza della persona autorizzata al trattamento.

E) USO DELLE CHIAVI E DEI BADGE MESSI A DISPOSIZIONE DA XXXX

Il referente autorizzato che riceve tali strumenti si impegna a proteggerli da furto, perdita, danneggiamento e, in ogni caso segnalare al Titolare del trattamento il furto, la perdita o il danneggiamento. È vietato lasciarli in luoghi incustoditi.

Il Titolare si riserva la facoltà di disabilitarne l'utilizzo/ritirare i mezzi resi disponibili. Tali mezzi, infatti, sono strumenti di lavoro messi a disposizione del dipendente/collaboratore al fine di consentirgli lo svolgimento della propria mansione ma, come tutti gli strumenti di lavoro, essi rimangono nella completa e totale disponibilità di Opera Universitaria di Trento

Alla cessazione del rapporto di lavoro gli strumenti vanno riconsegnati al Titolare del trattamento

F) SANZIONI

In caso venissero riscontrate azioni illecite o il mancato rispetto delle istruzioni contenute nel presente documento, il Titolare del trattamento si riserba di provvedere ad azioni disciplinari nei confronti del lavoratore a cui possono essere imputate (in maniera lampante) le predette azioni illecite, sempre e comunque secondo le regole previste dal C.C.N.L. e lo statuto dei lavoratori.

Trento, maggio 2018

Firma per accettazione della nomina

DATA
Firma per accettazione della nomina come persona autorizzata al Trattamento e come Referente privacy

_____

Il/La dipendente/collaboratore firmatario/a conferma di aver preso conoscenza del presente accordo come parte integrante del contratto di lavoro e di osservarne le disposizioni nello svolgimento del proprio lavoro.