# UNIVERSITA' DEGLI STUDI di GENOVA

## ATTO di AUTORIZZAZIONE al TRATTAMENTO DEI DATI PERSONALI E PATTO DI RISERVATEZZA

Ai sensi del Regolamento 2016/679 del Parlamento Europeo del Consiglio del 27 aprile 2016 "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" (*General Data Protection Regulation* –GDPR), rinvenibile al sito http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ITA&toc=OJ:L:2016:119:TOC ,

la S.V. è Autorizzata

al trattamento dei dati correlati alle attività che Lei svolge presso l'Università degli Studi di Genova, contenuti in atti e documenti riguardanti archivi di tipo cartaceo o banche dati elettroniche automatizzate.
A tal fine si riportano di seguito le istruzioni cui la S.V. dovrà attenersi per il trattamento dei dati di competenza, nel rispetto della normativa vigente in materia di protezione dei dati personali, evidenziando che la S.V. è tenuta a mantenere riservati e a non comunicare a terzi o diffondere le notizie, le informazioni, i dati appresi in conseguenza o anche solo in occasione dello svolgimento dei propri compiti istituzionali, ad eccezione dei casi in cui la legge preveda un obbligo di rivelare o riferire alle Pubbliche Autorità.

## ISTRUZIONI AGLI AUTORIZZATI del TRATTAMENTO DEI DATI PERSONALI

In ottemperanza alle disposizioni del Regolamento 2016/679 del Parlamento Europeo del Consiglio del 27 aprile 2016 "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" (*General Data Protection Regulation* –GDPR) ed in relazione alle attività svolte per l'Università degli Studi di Genova, l'"*Autorizzato",* dovrà effettuare i trattamenti di dati personali di competenza attenendosi scrupolosamente alle seguenti istruzioni ed ad ogni ulteriore indicazione che potrà essere fornita dal "Titolare", dal "Contitolare" o dal "Responsabile" del trattamento.

I dati personali devono essere trattati:

**a)** in osservanza dei criteri di riservatezza;
**b)** in modo lecito e secondo correttezza;
**c)** per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
**d)** nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Le misure minime di sicurezza (di cui alla sezione 2 del citato GDPR) sono obbligatorie e sono distinte in funzione delle seguenti modalità di trattamento dei dati:

1. **senza l'ausilio di strumenti elettronici** (es. dati in archivi cartacei o su supporto magnetico/ottico);
2. **con strumenti elettronici**

### 1. TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.

#### 1.1 Custodia

- I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non autorizzate al trattamento (es. armadi o cassetti chiusi a chiave).
- I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

**1.2 Comunicazione**

- I dati personali non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie attività svolte nell'ambito dell'Ateneo (anche se queste persone sono a loro volta autorizzate al trattamento). I dati non devono essere comunicati all'esterno dell'Università e comunque a soggetti terzi se non previa autorizzazione.

**1.3 Distruzione**

- Qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.
- I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti.

**1.4 Ulteriori istruzioni in caso di trattamento di categorie particolari di dati**

- I documenti contenenti dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale nonché dati genetici, dati biometrici intesi ad indentificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona devono essere custoditi e trattati dagli Autorizzati in modo che non vi accedano persone prive di autorizzazione nel rispetto delle previsione di cui all'art. 9 del GDPR.

- L'archiviazione dei documenti cartacei contenenti i predetti dati deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.
- Per accedere agli archivi contenenti categorie particolari di dati personali fuori orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure farsi identificare e registrare su appositi registri.

## 2. TRATTAMENTI CON STRUMENTI ELETTRONICI

**2.1 Protezione degli strumenti elettronici (ad esempio Pc, Smartphone, tablet,..) e dei dati**

- Tutti gli strumenti e applicazioni informatiche, dati in uso dall'Ateneo, devono essere dotate di *password*, ove possibile.
- Tutti gli strumenti elettronici devono essere dotati di *software antivirus*, aggiornato.
- I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
- Sui personal computer, notebook,… devono essere installati esclusivamente *software* necessari all'attività svolta nell'ambito dell'Ateneo e dotati di licenza.
- Per evitare accessi illeciti, deve essere sempre attivato il salva schermo con *password*.
- Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
- Nel caso in cui dati personali vengano trattati e archiviati unicamente sul dispositivo elettronico assegnato in uso (cioè non accessibili tramite i sistemi informatici universitari), l'autorizzato provvede al relativo back-up, per il tempo strettamente necessario alla finalità del trattamento.
- I supporti di memoria utilizzati per il *back-up* devono essere trattati secondo le regole definite al punto "Trattamento senza l'ausilio di strumenti elettronici".

**2.2 Gestione delle credenziali di autenticazione**

- L'accesso alle procedure informatiche che trattano dati personali è consentito agli Autorizzati in possesso di "credenziali di autenticazione" che permettano il superamento di una procedura di riconoscimento. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Autorizzato (*user-id*) associato ad una parola chiave riservata (password), oppure in un dispositivo di autenticazione (es. *smart card*) o in una caratteristica biometrica. Gli Autorizzati devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni:

- Le *user-id* individuali per l'accesso alle applicazioni non devono mai essere condivise tra più utenti (anche se Autorizzati al trattamento). Nel caso altri utenti debbano poter accedere ai dati è necessario richiedere l'autorizzazione al Responsabile del trattamento.
- Gli strumenti di autenticazione (ad esempio le password) che consentono l'accesso alle applicazioni devono essere mantenute riservate. Essi non vanno mai condivisi con altri utenti (anche se Autorizzati al trattamento).
- Le password devono essere sostituite, a cura del singolo Autorizzato, al primo utilizzo e successivamente almeno ogni sei mesi.
- Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
- Le password devono essere composte nel rispetto delle seguenti istruzioni:
  - Usare almeno 8 caratteri o usare un numero di caratteri pari al massimo consentito.
  - Usare lettere, numeri e almeno un carattere, a titolo esemplificativo ***; ? $ ! @ - >***<
  - Non utilizzare date di nascita, nomi o cognomi propri o di parenti
  - Non sceglierla uguale alla matricola o alla user-id
  - Custodirla sempre in un luogo sicuro e non accessibile a terzi
  - Non divulgarla a terzi
  - Non condividerla con altri utenti

**2.3 Cancellazione dei dati dai dispositivi elettronici**

- I dati personali conservati sui PC e su altri dispositivi elettronici devono essere cancellati in modo sicuro.

**2.4 Conservazione**

- I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

**2.5 Ulteriori istruzioni in caso di trattamento di categorie particolari di dati**

- Le *password* di accesso alle procedure informatiche che trattano i casi particolari di dati elencati al punto 1.4 devono essere sostituite, da parte del singolo autorizzato, almeno ogni tre mesi.
- L'installazione degli aggiornamenti *software* necessari a prevenire vulnerabilità e correggerne i difetti deve essere effettuato almeno semestralmente.

## 3. ISTRUZIONI DI CARATTERE GENERALE

**Come comportarsi in presenza di ospiti o di personale di servizio**

- Fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.
- Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salvaschermo del strumento elettronico.
- Non rivelare ad altri le password.
- Segnalare qualsiasi anomalia al Responsabile ovvero al Titolare, o al Contitolare.

**Come gestire la posta elettronica**

- Non aprire messaggi con allegati di cui non si conosce l'origine.
- Evitare di aprire filmati e presentazioni non attinenti l'attività lavorativa per evitare situazioni di pericolo per i dati contenuti sul vostro strumento elettronico.

**Come usare correttamente Internet**

- Evitare di scaricare dalla rete file e software di uso non direttamente riferibile all'attività svolta nell'ambito dell'Ateneo, in quanto questo può rendere vulnerabili i sistemi.
- Non leggere le caselle personali esterne se non si è certi che il provider esterno attui tutte le misure di sicurezza previste dalla normativa, in particolare nei riguardi dei virus informatici.

**4. SANZIONI PER INOSSERVANZA DELLE NORME**

Le presenti istruzioni sono impartite ai sensi delle normative vigenti in materia di protezione dei dati personali, l'inosservanza delle quali da parte dell'Autorizzato può comportare sanzioni anche di natura penale a suo carico.

Il Direttore Generale
Contitolare del Trattamento
*Firmato digitalmente*

Il Rettore
Titolare del trattamento
*Firmato digitalmente*