La protezione dei dati personali
Attuazione del Regolamento UE 2016/679 e del D.Lgs. n. 196/2003 e ss.mm.ii.

MANUALE AD USO DEI REFERENTI E DEGLI AUTORIZZATI

Versione: 2022
Numero totale pagine: 35

ELENCO DEI CONTENUTI

ELENCO DELLE TABELLE

MANUALE AD USO DEI REFERENTI E DEGLI AUTORIZZATI

1. INDICAZIONI GENERALI PER IL TRATTAMENTO DI DATI PERSONALI

1.1. I principi e gli obblighi fondamentali

Il primo gennaio del 2004 è entrato in vigore il decreto legislativo 30 giugno 2003, n. 196, recante il "**Codice in materia di protezione dei dati personali**" - d'ora in poi denominato "Codice" - nel quale sono raccolte, in forma di testo unico, tutte le disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali ed alle attività connesse. Il Codice sancisce il diritto alla protezione dei dati personali, prerogativa fondamentale della persona, e garantisce che il trattamento diqueste informazioni "si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".

Il sistema di garanzie approntato dal Codice si ispira ai principi di semplificazione, efficacia ed armonizzazione delle modalità di esercizio dei diritti e delle libertà fondamentali dell'interessato e degli adempimenti degli obblighi da parte dei titolari dei trattamenti *(art. 2, comma 2)*.

Il Codice introduce pertanto una simmetria tra le disposizioni che disciplinano:

a) le modalità d'esercizio dei diritti degli interessati
b) l'adempimento degli obblighi da parte del titolare del trattamento.

La normativa, dinamica e coerente con gli indirizzi giurisprudenziali più attuali, è improntata ai principi di:

- **Semplificazione**: nella ricerca di percorsi più snelli per le modalità di esercizio dei diritti da parte degli interessati e degli adempimenti da parte del titolare.
- **Armonizzazione**: nello sforzo di creare un sistema privacy pubblico-privato differenziato, ma coerente e di collegarsi in modo coordinato all'intero impianto legislativo vigente, non solo in materia di tutela della privacy.
- **Efficacia**: nel rendere il Codice concretamente operativo, mediante la previsione, accanto alle norme primarie (norme di legge), di norme secondarie di attuazione e di dettaglio (norme di regolamento).

Il diritto alla protezione dei dati personali potrà essere garantito solo se le amministrazioni titolari dei trattamenti ispireranno la loro attività ai principi sanciti dal Codice e conseguentemente, oltre ad ottemperare agli obblighi ivi espressamente previsti, adotteranno una serie di comportamenti concreti, azioni e provvedimenti organizzativi coerenti con i principi che regolano la materia.

A seguito dell'entrata in vigore del Regolamento UE 2016/679 vincolante per gli Stati europei, il Codice è stato modificato dal D.Lgs. n. 101/2018 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679, relativo alla protezione delle persone fisiche con riguardo al

trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Nel mese di ottobre del 2021 il Codice è stato ulteriormente modificato a seguito dell'emanazione del D.L. n. 139/2021 (cd. Decreto Capienze, convertito con modificazioni in L. n. 205/2021) ampliando in particolare le basi di liceità del trattamento per le Pubbliche Amministrazioni (cfr. art. 2-ter co. 1-bis del Codice) agli atti amministrativi generali.

1.2. Il significato di alcuni termini introdotti dalla normativa vigente

Il Regolamento UE 2016/679 definisce dato **personale** "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

Nei sistemi informativi di una organizzazione le informazioni contenenti dati personali sono presenti essenzialmente nelle seguenti forme:

- dati strutturati (ad esempio, database)
- dati destrutturati (ad esempio, documenti o posta elettronica).

È fondamentale comprendere che la norma protegge i dati personali indipendentemente dalla forma nella quale essi sono organizzati e del supporto utilizzato (sia questo informatico o meno).

I dati personali rientranti nella tipologia delle **categorie particolari di dati** sono quelli idonei a rivelare *l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici e biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona* (art. 9 par. 1 del Regolamento UE 2016/679). Pertanto, nell'ambito dell'Ateneo, le categorie particolari di dati personali concretamente utilizzati sono relativi a:

- appartenenza del dipendente ad associazioni sindacali;
- inabilità del dipendente;
- inabilità del familiare del dipendente;
- malattia del dipendente;
- provvedimenti giudiziari a carico del dipendente;
- handicap dello studente.

I dati personali relativi a **condanne penali e reati** (art. 10 del Regolamento UE 2016/679) sono quelli idonei a rivelare *provvedimenti di iscrizione nel casellario giudiziale o nell'anagrafe delle sanzioni amministrative dipendenti da reato e i relativi carichi pendenti, o la qualità di imputato o di indagato.*

Per **trattamento** deve intendersi qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio processi automatizzati e applicate a dati personali o insieme di dati personali, come la *raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto, l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4 par. 1 n. 2 del Regolamento UE 2016/679)*.

Il **titolare** 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4 par. 1 n. 7 del Regolamento UE 2016/679).

Il **responsabile del trattamento** è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4 par. 1 n. 8 del Regolamento UE 2016/679).

Il **referente del trattamento** è ciascuno dei soggetti di seguito elencati, ai quali, in virtù della specifica posizione organizzativa ricoperta, è assegnata la funzione e le responsabilità di referente del trattamento dei dati personali gestiti nell'ambito delle attività istituzionali di competenza, in attuazione di quanto previsto all'art. 2- quaterdecies del "*Codice in materia di protezione dei dati personali*", D. Lgs. n. 196/2003 e ss.mm.ii (art. 7 co. 1 del Regolamento di Ateneo in materia di trattamento dei Dati Personali emanato con D.R. n. 1226 del 19/03/2021– d'ora in poi denominato "Regolamento di Ateneo"):

a. i Dirigenti delle Ripartizioni;

b. i Capi Ufficio dell'amministrazione centrale;

c. i Capi Ufficio dei Dipartimenti e i Responsabili amministrativi dei Centri di Servizio, dei Centri di Ricerca, del Centro per le Biblioteche, dei Centri Museali, delle altre strutture assimilate;

d. i Direttori Tecnici delle strutture decentrate;

e. i Direttori dei Dipartimenti e dei Centri di Servizio, dei Centri di Ricerca, del Centro per le Biblioteche, dei Centri Museali, delle altre strutture assimilate;

f. i Presidenti delle Scuole;

g. i Responsabili amministrativi delle Scuole;

h. i professori e i ricercatori responsabili scientifici di progetti di ricerca, per quanto concerne il trattamento dei dati personali inerenti allo svolgimento della ricerca.

Gli **autorizzati** sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile (art. 29 del Regolamento UE 2016/679). Ai sensi dell'art. 8 del Regolamento di Ateneo, gli autorizzati dei trattamenti dei dati personali, anche delle categorie particolari di dati e di dati relativi a condanne penali e reati, effettuati dall'Università sono nominati dai Referenti tra il personale afferente all'ufficio o struttura.

L'**interessato** è la persona fisica, identificata o identificabile, a cui si riferiscono i dati personali (art. 4 par. 1 n. 1 del Regolamento UE 2016/679).

1.3. Indicazioni generali per il trattamento

Il trattamento dei dati personali da parte delle pubbliche amministrazioni è consentito solo qualora sia necessario per lo svolgimento delle funzioni istituzionali, rispettando gli eventuali altri presupposti e limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti.

Le categorie particolari di dati personali possono, invece, essere trattati soltanto se il trattamento risulta autorizzato da un'espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

Nell'effettuare qualsivoglia trattamento, al fine di mantenersi entro gli ambiti della legittimità fissati dal Codice, i referenti dovranno verificare che il trattamento si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale ed al diritto alla protezione dei dati personali. In particolare, ciascun trattamento dovrà essere effettuato riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante,rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

In ogni caso, i dati personali devono essere trattati:
- in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

1.4. Consenso e informativa

Si evidenzia che il Codice prevede che i soggetti pubblici e, dunque l'Università, salvo quanto espressamente previsto per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, non devono richiedere il consenso dell'interessato.

Il Codice prescrive inoltre l'obbligo di rendere l'informativa per tutti i trattamenti effettuati. Pertanto, il referente dovrà adottare ogni misura organizzativa idonea, ivi compresa la predisposizione di idonea informativa (secondo le prescrizioni degli artt. 12-14 del Regolamento UE 2016/679) come previsto nell'art. 7 "**Referenti del trattamento e compiti**" co. 2 lett. e) del Regolamento di Ateneo: "curare nell'ambito di propria competenza, la redazione e l'aggiornamento delle informative e comunicazioni da fornire all'interessato sul trattamento dei dati personali di cui agli artt. 12-14 del Regolamento UE 2016/679, da pubblicare nell'apposita pagina del sito web di Ateneo; a tal fine può avvalersi della collaborazione del Responsabile per la Protezione dei Dati di Ateneo (RPD) e dell'Ufficio privacy" e l'inserimento dell'informativa breve nella modulistica utilizzata nell'ambito della propria struttura, affinché l'interessato o la persona presso la quale sono raccolti i dati personali siano previamente informati per iscritto circa il trattamento dei dati.

Al fine di poter provare in ogni caso di **aver adempiuto all'obbligo di rendere l'informativa**, sebbene il Codice preveda la possibilità di renderla anche solo oralmente, **si dispone che la stessa venga resa sempre per iscritto**.

1.5. Diritti dell'interessato

L'interessato al trattamento ha diritto di richiedere all'Università degli Studi di Napoli Federico II, quale Titolare del trattamento, ai sensi degli artt. da 15 a 22 del Regolamento UE 679/2016:
- l'accesso ai propri dati personali ed a tutte le informazioni di cui all'art. 15 del Regolamento UE 2016/679;
- la rettifica dei propri dati personali inesatti e l'integrazione di quelli incompleti;
- la cancellazione dei dati personali (c.d. "**diritto all'oblio**"), fatta eccezione per quelli contenuti in atti che devono essere obbligatoriamente conservati dall'Università, in adempimento ad un obbligo di legge o per l'esecuzione dei propri compiti di interesse pubblico;
- la limitazione del trattamento ove ricorra una delle ipotesi di cui all'art. 18 del Regolamento UE 2016/679;
- l'opposizione al trattamento dei propri dati personali, salvo quanto previsto con riguardo alla necessità del trattamento dati per poter fruire del servizio offerto;
- la revoca del consenso eventualmente prestato, senza che ciò pregiudichi la liceità del trattamento basato sul consenso prima della revoca;
- la portabilità dei dati, ove ne ricorrano i presupposti, nelle ipotesi in cui la base giuridica del trattamento sia il consenso, anche al fine di comunicare tali dati a un altro Titolare del trattamento.

L'interessato ha il diritto di proporre reclami all'Autorità Garante per la Protezione dei dati personali nel caso ritenga che il trattamento dei dati che lo riguardi non sia conforme alle disposizioni vigenti ai sensi dell'art. 77 del Regolamento UE 2016/679 e di adire le opportune sedi giudiziarie per proporre ricorso ai sensi dell'art. 79 del Regolamento UE 2016/679.
Per l'esercizio dei diritti di tutela dei propri dati personali, l'interessato può rivolgersi al Titolare del trattamento, nella persona del Rettore p.t., e al Responsabile della Protezione dei Dati, utilizzando i seguenti contatti:
• Titolare del trattamento: Email: ateneo@unina.it PEC: ateneo@pec.unina.it
• Responsabile della Protezione dei Dati (RPD): Email: rpd@unina.it PEC: rpd@pec.unina.it

Quando la richiesta riguarda la mera richiesta di informazioni relative al trattamento eventualmente in atto, può essere formulata anche oralmente; in tal caso è annotata sinteticamente a cura del referente o dell'autorizzato.

Al fine di esaudire la richiesta dell'interessato il referente, o un autorizzato all'uopo individuato,dovrà:

- comunicare oralmente le informazioni richieste;

oppure

- consentire la visione delle informazioni mediante strumenti elettronici;

oppure

- se richiesto, provvedere alla trasposizione dei dati su supporto cartaceo o informatico ovveroall'invio per via telematica.

1.6. Comunicazione e diffusione di dati personali

La **comunicazione** e la **diffusione** di dati personali costituiscono trattamenti particolarmente delicati. Si ritiene utile, pertanto, richiamare l'attenzione dei referenti sulle disposizioni da osservare, coerentemente con quanto disposto dal Regolamento di Ateneo.

La comunicazione dei dati nell'ambito dell'Ateneo è ispirata al principio della libera circolazione delle informazioni. La comunicazione ad altro soggetto pubblico è invece ammessa o quando è prevista da una norma di legge o di regolamento o atti amministrativi generali oppure quando è comunque necessaria per lo svolgimento di funzioni istituzionali dell'ente richiedente.

Si riporta il testo dell'art. 15 "Comunicazione dei dati a soggetti pubblici e privati e diffusione" del Regolamento di Ateneo:

1. La richiesta di dati personali, diversi da quelli di cui alle categorie degli artt. 9 e 10 del Regolamento UE 2016/679, proveniente da soggetti pubblici o da privati, deve essere scritta e motivata.

2. I Referenti devono valutare la legittimazione del richiedente ad ottenere tali dati e ove sia positiva, autorizzare la visione o la trasmissione dei dati nella misura e secondo le modalità strettamente necessarie a soddisfare la richiesta.

3. E', in ogni caso, autorizzata la pubblicazione all'albo ufficiale, nonché sul sito web dell'Università, delle graduatorie relative a procedure concorsuali o concorrenziali, anche con riferimento ai risultati di prove selettive o valutazioni intermedie.

4. I dati vengono rilasciati a condizione che il richiedente si impegni a utilizzarli esclusivamente per le finalità e nell'ambito delle modalità indicate nelle richieste e si impegni ad adottare tutte le misure necessarie a garantirne la sicurezza, secondo quanto prescritto dalla normativa in materia di protezione dei dati personali.

La diffusione di categorie particolari di dati personali e dati personali relativi a condanne penali e reati non è mai ammessa (artt. 9 e 10 del Regolamento UE 2016/679). La diffusione di dati personalidiversi da quelli rientranti nelle categorie particolari di dati personali e di dati personali relativi a condanne penali e reati è invece ammessa unicamente quando sono previste da norma dilegge o di regolamento o di atti amministrativi generali, richiamando le quali il trattamento potrà essere effettuato. In ogni caso, i dati idonei a rivelare lo stato di salute non possono essere diffusi.

1.7. Le responsabilità e le sanzioni

Il Titolare del trattamento (l'Ateneo nelle persone del Rettore e del Direttore Generale, in riferimento alle relative competenze come individuate dalla Statuto di Ateneo) è competente per il rispetto dei principi applicabili al trattamento dei dati personali indicati all'art. 5 par. 1 del Regolamento UE 2016/679 e deve essere in grado di comprovarlo (principio di «responsabilizzazione»).

In base a questo principio, chiunque (referente o autorizzato, in relazione ai rispettivi ambiti di responsabilità) cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'*art. 2050 c.c. (responsabilità derivante dall'esercizio di attività pericolose)* se non prova di aver adottato tutte le misure tecniche ed organizzative idonee ad evitare il danno.

Al fine di poter fornire la prova di aver adottato tutte le misure tecniche ed organizzative idonee ad evitare il danno, risulta indispensabile per i referenti e per gli autorizzati di trattamento osservare scrupolosamente le istruzioni individuate dal Titolare in attuazione della normativa in materia di protezione dei dati personali.

Si evidenzia, altresì, che, in ogni caso, la violazione di disposizioni del Titolare costituisce violazione dei doveri d'ufficio ed implica, conseguentemente l'applicabilità di sanzioni disciplinari.

Si riporta di seguito il testo dell'art. 26 "Violazioni" del Regolamento di Ateneo:
1. Le violazioni delle disposizioni del presente Regolamento in materia di trattamento dei dati personali e del Regolamento UE 2016/679, costituiscono violazioni degli obblighi di comportamento e saranno valutate quali ipotesi di responsabilità disciplinare secondo i principi e le modalità previste dagli specifici codici etici e di disciplina.
2. Delle intervenute violazioni sarà altresì presentata denuncia alle Autorità competenti ove appaiano configurarsi ipotesi di responsabilità civile, penale o amministrativa.

Riguardo le sanzioni, si riporta di seguito il testo dell'art. 167 del Codice:

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2 sexies e 2 octies, o delle misure di garanzia di cui all'articolo 2 septies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni.

3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.

Fra le tante sanzioni previste dal Codice si ritiene inoltre opportuno, segnalare che:

- la omessa o inidonea informativa all'interessato, la cessione di dati al di fuori dei casi consentiti, la violazione delle disposizioni in tema di comunicazione di dati personali idonei a rivelare lo stato di salute o la vita sessuale nonché l'omessa informazione o esibizione di documenti al Garante comportano l'applicabilità di una sanzione amministrativa;
- il trattamento illecito di dati, la falsa notifica o false informazioni al Garante, l'omessa adozione delle misure minime di sicurezza e l'inosservanza dei provvedimenti del Garante costituiscono per il trasgressore illecito penale;
- come pena accessoria è sempre prevista la pubblicazione della sentenza di condanna.

1.8. Sicurezza dei dati e dei sistemi

Ai sensi dell'art. 33 e dell'art. 34 del Codice, il trattamento dei dati personali è consentito solo se sono adottate le misure di sicurezza, distinte a seconda che il trattamento sia effettuato con o senza l'ausilio di strumenti elettronici:

1.8.1. Trattamenti effettuati con l'ausilio di strumenti elettronici

a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico (**almeno annuale**) dell'individuazione dell'ambito del trattamento consentito ai singoli autorizzati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza fuori linea, il ripristino della disponibilità dei dati edei sistemi;
g) adozione di tecniche di offuscamento o di codici identificativi per determinati trattamenti di dati idonei arivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

1.8.2. Trattamenti effettuati senza l'ausilio di strumenti elettronici

a) aggiornamento periodico (**almeno annuale**) dell'individuazione dell'ambito del trattamento consentito ai singoli autorizzati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli autorizzati per lo svolgimento dei relativi compiti;

c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli autorizzati.

L'adozione di misure di sicurezza inadeguate (cioè non coerenti con quanto disciplinato dal Codice o dalla legge) rende il trattamento illecito, per cui il titolare non può più utilizzare i dati raccolti e l'interessato può ottenerne la cancellazione.

2. GLI ADEMPIMENTI PER IL REFERENTE

2.1. La nomina degli autorizzati

Qualora siano gestiti dati **personali**, il referente del trattamento dei dati dovrà autorizzare per iscritto gli autorizzati procedendo alla revoca della detta autorizzazione in tutti i casi di perdita della qualità che consente all'autorizzato l'accesso ai dati personali (per es.: per trasferimento del dipendente ad altro ufficio, per assegnazione ad altre attività, per estinzione del rapporto di lavoro con l'Ateneo).

Per il conferimento e la revoca dell'incarico, il referente dovrà utilizzare:

a. i modelli SICURDAT/A per autorizzare i trattamenti effettuati tramite PC con procedure non centralizzate, con procedure esterne e con archivi non automatizzati (cartacei);
b. il modello SICURDAT/B per autorizzare i trattamenti automatizzati centralizzati.

In ogni caso, sul modulo dovrà essere apposta anche la firma dell'autorizzato del trattamento per attestare l'avvenuta comunicazione della designazione a lui affidata e dell'ambito di trattamento che gli è consentito. I due modelli SICURDAT sono reperibili all'indirizzo: https://www.unina.it/ateneo/statuto-e-normativa/privacy.

Gli uffici dell'Amministrazione Centrale e delle Strutture autonome dovranno protocollare ed inviare senza nota di trasmissione – esclusivamente tramite Protocollo Informatico – tali moduli all' Ufficio Privacy, custodendo gli originali. Per motivi di organizzazione interna, è opportuno effettuare registrazioni di protocollo separate per i modelli SICURDAT/A e SICURDAT/B.

Per quanto attiene alle strutture di Ateneo, la gestione e la conservazione dei moduli SICURDAT è regolamentata da appositi decreti e comunicazioni del titolare ai referenti.

Nel caso di comunicazione all'esterno dell'Ateneo di dati personali (mediante trasmissione di flusso cartaceo o elettronico, oppure mediante l'utilizzo di specifiche applicazioni informatiche non gestite centralmente dall'Ateneo) si evidenzia l'importanza di segnalare, nei modelli SICURDAT/A, la denominazione dei soggetti o degli enti esterni a cui i dati sono comunicati e dell'applicazione utilizzata. Il referente deve segnalare queste informazioni anche nel caso di accesso a banche dati esterne gestite da applicazioni informatiche dell'ente o soggetto esterno.

All'atto del conferimento dell'autorizzazione, il referente deve mettere a disposizione all'autorizzato il presente manuale
(reperibile anche all'indirizzo: https://www.unina.it/ateneo/statuto-e-normativa/privacy), in quantocontiene - tra l'altro - le istruzioni, le regole e le prassi a cui devono attenersi gli autorizzati per la tutela dei dati personali trattati dall'Università degli Studi di Napoli Federico II.

2.2. L'aggiornamento dell'ambito di trattamento

Con frequenza annuale, ciascun referente deve provvedere a comunicare all'Ufficio Privacy a mezzo degli appositi modelli Sicurdat eventuali variazioni della situazione di fatto esistente nella struttura stessa (o

ufficio), al fine di evitare la violazione della normativa vigente per quanto attiene alla erronea individuazione dell'ambito di trattamento consentito ai referenti ed agli autorizzati.

2.3. L'informativa

Ai sensi di quanto è prescritto dall'art. 7 "Referenti del trattamento e compiti" co. 2 lett. e) del Regolamento di Ateneo, l'informativa di cui agli artt. 12-14 del Regolamento UE 2016/679 è a cura del referente del trattamento ed è resa all'interessato direttamente ovvero è effettuata con modalità idonee a garantire ampia diffusione della stessa.

L'informativa relativa al trattamento di categorie particolari di dati personali e dati personali relativi a condanne penali e reati (artt. 9 e 10 del Regolamento UE 2016/679) deve contenere l'indicazione della normativa che prevede gli obblighi o i compiti in base alla quale il trattamento è effettuato. Inoltre, l'informativa relativa alla comunicazione e/o diffusione di dati personali deve essere sempre effettuata prima della trasmissione dei dati oggetto di trattamento.

In ogni caso, il referente è tenuto a conservare i documenti dai quali possa desumersi che l'informativa è stata resa in conformità alle disposizioni contenute nel Regolamento UE 2017/679 nonché nel Regolamento di Ateneo.

2.4. L'adozione delle misure di sicurezza

Al fine di garantire la sicurezza dei dati, il referente custodisce i dati seguendo le indicazioni che gli vengono fornite dal Titolare ed adottando ogni altra misura di sicurezza idonea a ridurre al minimo i rischi di distruzione, di perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. A tal fine, impartisce le opportune istruzioniagli autorizzati e vigila sul corretto svolgimento dei trattamenti di propria competenza.

Più specificatamente, il referente dovrà accertare, per lo svolgimento dei trattamenti di propria competenza, che sono garantite idonee soluzioni quali:

a) la disponibilità e l'utilizzo da parte degli autorizzati di un idoneo sistema di autenticazione;
b) la attenta custodia delle credenziali di autenticazione degli autorizzati;

c)la sicurezza del software e dell'hardware utilizzato dagli autorizzati in termini di: manutenzione, installazione di prodotti di protezione dei sistemi, di prevenzione delle vulnerabilità e di correzione, strumenti e procedure per il salvataggio periodico dei dati.

2.5. Il Documento Programmatico sulla Sicurezza (DPS) *[misura abrogata a seguito dell'entrata in vigore del Codice, ma consigliata come buona prassi]*.

Ciascun referente di trattamento dei dati personali, referente di struttura didattica, di ricerca o di servizio,

delle Strutture autonome (Dipartimento, Centro Interdipartimentale di Servizio o di Ricerca, Scuola di Specializzazione, Biblioteca, Centro di Ateneo, etc.) redige annualmente il Documento Programmatico sulla Sicurezza relativo al trattamento dei dati personali effettuati nel proprio ambito, eventualmente su schemi- tipo forniti dal Titolare ed avvalendosi dei contributi forniti dai referenti del trattamento dei dati personali, ove presenti, di sotto-strutture afferenti alla struttura stessa.

E' opportuno ricordare che la tenuta di un aggiornato DPS è tra le misure minime previste per i trattamenti automatizzati. Ai sensi dell'articolo 19 dell'allegato B del Codice, il DPS deve contenere:

- il censimento dei trattamenti di dati personali svolti (Reg. 19.1);
- l'analisi della distribuzione dei compiti e delle responsabilità (Reg. 19.2);
- l'analisi dei rischi incombenti sui dati (Reg. 19.3);
- la descrizione delle misure di garanzia adottate per l'integrità e la disponibilità dei dati, la protezione dei locali e delle aree (Reg. 19.4);
- la descrizione dei criteri e modalità per il ripristino dei dati a seguito di distruzione o danneggiamento, entro sette giorni nel caso di dati categorie particolari di dati personali e dati personali relativi a condanne penali e reati (Reg. 19.5);
- la previsione di interventi formativi a beneficio degli autorizzati (Reg. 19.6);
- la descrizione dei criteri per l'affidamento di elaborazioni dati all'esterno della struttura del Titolare (Reg. 19.7);
- la descrizione dei criteri per l'offuscamento o la separazione di dati idonei a rivelare lo stato di salute e lavita sessuale dagli altri dati personali dell'interessato (Reg. 19.8).

3. MISURE DI SICUREZZA IN FEDERICO II

3.1 Premessa

Le **"misure minime"** sono costituite, in accordo con quanto precedentemente detto, da quel complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali che l'Ateneo è tenuto ad adottare per ridurre al minimo i rischi di distruzione o di perdita, anche accidentale, dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta e che configurano il livello minimo di protezione richiesto dal Decreto Legislativo 196/2003 e ss.mm.ii. in materia di protezione dei dati personali.

Poiché il trattamento di dati personali può essere effettuato sia attraverso sistemi automatizzati sia attraverso supporti cartacei, è necessario distinguere tra:

1) Trattamenti automatizzati (effettuati con strumenti informatici e telematici)
2) Trattamenti non automatizzati (cartacei).

La presente guida, coerentemente con le misure minime definite nel Codice e con quanto prescritto nel Regolamento di Ateneo, contiene – tra l'altro – le istruzioni, le regole e le prassi a cui devono attenersi i referenti e gli autorizzati per la tutela dei dati personali trattati dall'Università degli Studi di Napoli Federico II.

Infine, è opportuno precisare che per tutto ciò che non è specificato nel presente manuale, il referente e l'autorizzato osservano:

1) il Regolamento UE 2016/679;
2) i principi contenuti nel D. Lgs. 196/2003 *Codice in materia di protezione dei dati personali e ss.mm.ii;*
3) il *Regolamento di Ateneo in materia di trattamento dei Dati Personali* adottato con D.R. n. 1226 del 19.03.2021;
4) Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. n. 101/2018;

3.2 Trattamenti automatizzati

Nell'ambito di tali trattamenti è necessario distinguere tra:

a) PC **non** collegati in rete;
b) PC collegati in rete ma **non** utilizzanti applicazioni informatiche centralizzate;
c) PC collegati in rete ed utilizzanti le applicazioni informatiche centralizzate.

3.2.1 Adempimenti di carattere generale previsti per tutte le tipologie di PC

3.2.1.1 Il sistema di autenticazione

L'autenticazione[2] fa riferimento alla capacità di un determinato sistema di consentire ad un utente autorizzato di accedere ai servizi ed alle informazioni cui ha legittimamente diritto e, contemporaneamente,

[2] Definizione: un sistema di autenticazione è un dispositivo atto a stabilire e verificare in modo univoco, anche indiretto, l'identità dichiarata da un utente che vuole accedere al sistema, prima di ulteriori interazioni tra il sistema e l'utente.

di impedire qualunque tipo di accesso a chi, invece, non ha le autorizzazioni necessarie. L'applicazione di questo principio, ovviamente, comporta che il sistema debba essere in grado di memorizzare in modo sicuro le credenziali di ogni utente, di riconoscerlo all'atto della richiesta di un determinato servizio e di garantire che non possano avvenire manipolazioni delle richieste di accesso.

Tutti i PC devono essere accessibili attraverso l'utilizzo di un sistema di autenticazione, mediante l'utilizzo di password da inserire all'atto dell'accensione della macchina. I meccanismi da implementare dipendono dalla tipologia di PC (se collegato in rete locale, oppure no), dalle caratteristiche tecniche del PCe dalla disponibilità di idonee infrastrutture di servizio (ad esempio, la presenza di un sistema centralizzato per l'autenticazione). Tali aspetti saranno più diffusamente trattati nei prossimi paragrafi.

3.2.1.2 *La segretezza e la custodia della password*

Si sottolinea che l'attenta custodia della password di accensione va effettuata anche nell'interesse dello stesso utente al fine di non esporsi a dover rispondere di attività illecite svolte da altri soggetti tramite il PC a lui assegnato e dalla propria utenza.

Solo nel caso in cui sia indispensabile utilizzare uno specifico PC assegnato ad un dipendente in sua assenza (perché utilizzato per un particolare trattamento di dati personali), il dipendente dovrà aver cura di consegnare al referente del trattamento dati in busta chiusa la password di quel PC. Il referente del trattamento dei dati, in caso di impedimento temporaneo del dipendente aprirà la busta contenente la password e la fornirà ad altro dipendente per consentirglil'utilizzo del detto PC. La busta, con l'indicazione della data della sua apertura, dovrà essere conservata a cura del Referente fino alla consegna della busta contenente la nuova password da parte del dipendente che è stato temporaneamente impedito.

Il Referente è tenuto, inoltre, a verificare la corretta applicazione delle disposizioni relative alla password di accensione del PC oggetto di trattamento dei dati personali, riscontrando in particolare la sostituzione delle password (vale a dire delle buste contenenti le stesse).

3.2.1.3 Sicurezza del software e dell'hardware

Se nell'utilizzo del PC e/o dell'applicazione informatica a cui si è abilitati, viene rilevato un problema che può compromettere la sicurezza dei dati, l'autorizzato lo disconnette dalla rete e ne dà immediata comunicazione al referente del trattamento che, a sua volta, provvede ad attivare la ditta o la struttura di Ateneo preposta alla manutenzione dei PC che analizzerà il problema segnalato ed adotterà tutte le misure tecniche necessarie a risolverlo. Nel caso dell'Amministrazione Centrale, la struttura incaricata della manutenzione dei posti di lavoro è il CSI che sarà attivato dal referente mediante Contact Center all'indirizzo mail contactcenter@unina.it).

All'utente è vietato installare programmi non attinenti le normali attività d'ufficio, né nuovi programmi necessari, né modificare le configurazioni hardware e software delle apparecchiature, senza la preventiva autorizzazione della struttura di gestione (del CSI per l'amministrazione Centrale).

Gli utenti se rilevano la presenza di segnalazioni di correzioni software per problemi di sicurezza (aggiornamenti critici, aggiornamento Antivirus), sono tenuti a scaricare ed installare tali aggiornamenti sulla propria postazione di lavoro, seguendo le istruzioni impartite dal fornitore. Tale adempimento è applicabile a tutti gli utenti le cui postazioni di lavoro sono collegate alla rete internet. Per i PC non in rete, l'aggiornamento dovrà essere eseguito fuori linea.

Tutti gli autorizzati evitano qualsiasi tipo di azione teso a superare le protezioni applicate ai sistemi e alle applicazioni. Qualora l'intervento di installazione, configurazione e regolazione del sistema è effettuato da una ditta esterna o da personale di Ateneo preposto alla manutenzione dei PC (nel caso dell'Amministrazione Centrale dal CSI), a conclusione dell'intervento di manutenzione, il Referente del trattamento è tenuto comunque a verificare che il PC sia riportato nella situazione originaria per quanto riguarda le misure minime (password di accensione del PC, presenza del programma antivirus). È inoltrenon superfluo far presente che, qualora la manutenzione sia affidata ad una ditta esterna, questa deve essere formalmente nominata incaricata del trattamento.

È espressamente vietata qualsiasi azione volta a superare il blocco con password all'accensione del PC.

3.2.1.4 Protezione da virus informatici

I virus informatici rappresentano una delle minacce principali per la sicurezza dei sistemi informativi e dei dati in essi presenti. Un virus informatico può danneggiare un PC, può modificare e/o cancellare i dati in esso contenuti, può compromettere la sicurezza e la riservatezza di un intero sistema informativo, può rendere indisponibili parti del sistema informativo, ivi compresa la rete di trasmissione dati.

I seguenti comportamenti inducono un aumento del livello di rischio di contaminazione da virus informatici:

1) installazione di software gratuito (freeware o shareware) prelevato da siti internet o allegato a riviste e/o libri;
2) scambio di file eseguibili allegati a messaggi di posta elettronica;
3) ricezione ed esecuzione di file eseguibili allegati a messaggi di posta elettronica;
4) collegamenti ad internet con esecuzione di file eseguibili, applets Java, ActiveX;
5) utilizzo della condivisione, senza password, di cartelle fra computer in rete;
6) utilizzo di dispositivi di memoria esterna (penne USB) già utilizzati e la cui provenienza sia dubbia.

Al fine di evitare i problemi correlati alla diffusione di virus informatici, il referente e gli autorizzati si attengono alle istruzioni di seguito riportate:

1) accertarsi che sul proprio computer sia sempre operativo uno dei programmi antivirus in uso presso l'Ateneo. Nel caso contrario segnalare immediatamente la situazione alla ditta o alla struttura di Ateneo preposta alla manutenzione dei PC (nel caso dell'Amministrazione Centrale al CSI, tramite l'indirizzo mail contactcenter@unina.it);
2) aggiornare il programma antivirus, per i PC collegati in rete, automaticamente o su richiesta dell'utente. Per i PC non collegati in rete l'aggiornamento del programma antivirus deve essere effettuato con cadenza almeno mensile;
3) utilizzare sui PC esclusivamente la posta elettronica di Ateneo preferibilmente via web client dell'area riservata ed evitare di utilizzare redirezioni della stessa per l'utilizzo di altri client (ad esempio reindirizzare la posta Unina su GMAIL); accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati. Nel caso che il mittente del messaggio di posta elettronica dia origine a dubbi, inoltrare email a antispam@unina.it e cancellare direttamente il messaggio senza aprire gli allegati;

4) sottoporre a controllo, con il programma antivirus installato sul proprio PC, tutti i supporti di provenienza esterna e/o incerti prima di eseguire uno qualsiasi dei files in esso contenuti;
5) non condividere con altri computer il proprio disco rigido ed utilizzare esclusivamente gli strumenti messi a disposizione dell'Ateneo (p.e. Onedrive365, Collabora)
6) proteggere in scrittura i propri dispositivi di memoria esterna contenenti programmi eseguibili e/o files di dati;
7) evitare tassativamente la trasmissione fra computer in rete di files o cartelle di rete o procedure non autorizzate (le cartelle di rete per l'amministrazione centrale sono sostituite dal cloud privato Collabora; in mancanza del collegamento fare richiesta al CSI tramite contactcenter: contactcenter@unina.it)
8) non intraprendere azioni di modifica sui sistemi utilizzati a seguito di diffusione di messaggi e segnalazioni di virus informatici da qualsiasi fonte provengano. Le uniche azioni eventualmente necessarie sono comunicate esclusivamente dal CSI;
9) non scaricare dalla rete internet programmi o files non inerenti all'attività dell'Ufficio o comunque sospetti;
10) distribuire preferibilmente documenti in formato elettronico tramite formati standard, compatibili e possibilmente compressi (ad es. PDF).

Il Referente del trattamento dei dati della struttura è tenuto a verificare la corretta applicazione delle presenti disposizioni, accertando che tutti i PC dell'Ufficio siano dotati del programma antivirus. Nel caso riscontri la mancanza di tali protezioni minime, il referente è tenuto a far attivare il necessario intervento tecnico (nel caso dell'Amministrazione Centrale, contattando il Contact Center del CSI all'indirizzo mail contactcenter@unina.it).

Nel caso in cui da parte del programma antivirus sia riscontrata la presenza di un virus informatico sul PC, l'Autorizzato segue le istruzioni riportate sullo schermo dal programma e contestualmente avverte dell'evento il referente del trattamento dei dati Nel caso di persistenza della segnalazione di presenza di virus spegnere immediatamente il PC; nel caso di collegamento in rete staccarlo dalla rete e provvedere immediatamente a segnalare l'evento per eventuali e successivi interventi tecnici alla ditta o alla struttura di Ateneo preposta alla manutenzione dei PC (nel caso dell'Amministrazione Centrale contattando il Contact Center del CSI all'indirizzo mail contactcenter@unina.it).

3.2.1.5 Salvataggio periodico dei dati

Per garantire la disponibilità dei dati personali trattati con PC, a meno di meccanismi di salvataggio centralizzati (ma solo per i PC di tipologia b) e c)), il Referente è tenuto a verificare che, con cadenza almeno settimanale, tali dati siano archiviati su supporti di memorizzazione rimovibili (PENDRIVE-CHIAVETTA USB, CDROM, DVD) e che tali supporti siano conservati in armadi o cassetti muniti di serratura, secondo quanto specificato al successivo paragrafo 3.3.

3.2.2 *Adempimenti specifici previsti per il caso a) – PC non collegati in rete*

Per i PC non collegati in rete, il meccanismo per l'autenticazione deve essere necessariamente implementato in locale, sul PC.

Se sul PC è installato un sistema della famiglia Microsoft Windows che non prevede un sistema di autenticazione "nativo", la password di accensione deve essere in tal caso necessariamente da BIOS. La lunghezza minima della password è di 8 caratteri, o comunque del massimo consentito dal BIOS del PC; la password BIOS deve essere modificabile dall'autorizzato e variata almeno ogni sei mesi. Nel caso in cui sul PC risiedano categorie particolari di dati personali o dati personali relativi a condanne penali e reati (artt. 9 e 10 del Regolamento UE 2016/679), tale password deve essere modificata dall'autorizzato almeno ogni tre mesi.

Di seguito, le regole valide per l'utilizzo della password BIOS:

DESCRIZIONE	REGOLA
La password di BIOS può essere modificata dall'utente?	SI
Quale deve essere la durata della password di BIOS?	6 mesi oppure 3 mesi nel caso di trattamenti di categorie particolari di dati o dati personali relative a condanne penali e reati (artt. 9 e 10 del Regolamento UE 2016/679)
La password viene revocata in caso di mancato utilizzo?	NO
La password ha una lunghezza minima?	SI, 8 caratteri o comunque il massimo numero di caratteri consentiti dal BIOS del PC

Tabella 1 – Regole da implementare per l'utilizzo della password di BIOS

I PC più recenti, (MAC OS, Windows X) sono invece dotati di sistemi di autenticazione ed autorizzazione completi che permettono non solo l'utilizzo di user-id e password, ma anche di credenziali di autenticazione "forte" quali token o device di riconoscimento biometrico. L'utilizzo dell'autenticazione "locale" non esclude l'adozione anche della password BIOS.

Di seguito, le regole valide per l'utilizzo della password locale del PC:

DESCRIZIONE	REGOLA
La password locale del PC può essere modificata dall'utente?	SI
Quale deve essere la durata della password locale del PC?	6 mesi oppure 3 mesi nel caso di trattamenti di categorie particolari di dati o dati personali relative a condanne penali e reati
La password viene revocata in caso di mancato utilizzo?	NO
La password deve avere una lunghezza minima?	SI, almeno 8 caratteri

Tabella 2 – Regole da implementare per l'utilizzo della password locale del PC

Per quanto attiene alle restanti misure minime di sicurezza, gli autorizzati provvedono ad eseguire:

- con cadenza almeno mensile, da disco rimovibile, l'aggiornamento del sistema operativo presente sul proprio PC e del programma antivirus;
- con cadenza almeno settimanale, al salvataggio dei propri dati personali su supporti dimemorizzazione rimovibili (PENDRIVE-CHIAVETTA USB, CDROM, DVD) che devono essere conservati in armadi o cassetti muniti di serratura, secondo quanto specificato al successivo paragrafo 3.3;
- ad impostare la protezione mediante screen-saver con password.

È opportuno evidenziare, infine, che i trattamenti eseguiti sui PC non collegati in rete devono essere autorizzati mediante moduli SICURDAT/A.

3.2.3 *Adempimenti specifici previsti per il caso b) – PC collegati in rete ma non alle applicazioni centralizzate*

Se il PC è collegato alla rete locale, l'autenticazione deve essere preferibilmente gestita da un sistema centralizzato di autenticazione. In tal caso, la password deve essere di lunghezza non inferiore a 8 caratteri o, comunque, al massimo numero di caratteri consentiti dal sistema di autenticazione utilizzato.

L'utilizzo di un sistema centralizzato di autenticazione, in generale, permette:

- la protezione e la gestione delle password (lunghezza minima, scadenza della password, rinnovo della password, cessazione dell'utenza, regole di composizione della password, ecc.) grazie ad un'unica procedura di accesso alle risorse di rete
- la profilatura utente grazie all'impostazione di privilegi per il controllo dell'accesso agli oggetti della directory e ai singoli elementi dati che li costituiscono
- la gestione della sicurezza anche dei sistemi client collegati
- la sicurezza nell'accesso ad Internet attraverso il supporto per i protocolli sicuri standard di Internet ed i meccanismi di autenticazione degli utenti quali Kerberos, PKI (Public Key Infrastructure) e MFA Multi Factor Authentication
- la pre-impostazione centralizzata della protezione mediante screen-saver
- gestione della lista degli autorizzati al trattamento dei dati in relazione al profilo di autorizzazione ed al conseguente ambito di trattamento consentito.

Sul mercato sono disponibili diverse soluzioni tecnologiche, alcune in ambiente Open Source (Developers Italia), atte a garantire i requisiti di sicurezza precedentemente esposti. Sarà cura del referente individuare ed adottare la soluzione più idonea per la propria struttura. E' possibile collegare i PC anche a sistemi di autenticazione bastati su protocolli tipo OpenID sfruttando l'autenticazione con CIE e/o SPID.

Per l'**Amministrazione Centrale**, il sistema di autenticazione è un sistema complesso di Single Sign On: la password del PC risiede su un server di dominio per il controllo di autorizzazione gestito dal CSI. La password di rete scade automaticamente ogni sei mesi e le credenziali sono disattivate. Dopo cinque tentativi di connessione falliti, il codice identificativo (userid) è disabilitato. La richiesta di riabilitazione è effettuata dall'autorizzato, tramite il Contact Center del CSI all'indirizzo mail contactcenter@unina.it).

Di seguito, le regole da implementare su di un qualunque server di dominio ed attualmente impostate da CSI sul sistema di SSO che gestisce l'autenticazione alla rete per i PC dell'Amministrazione. Tali regole si applicano anche per i PC di tipologia c): PC collegati in rete ed utilizzanti le applicazioni informatiche centralizzate.

DESCRIZIONE	REGOLA
La password locale del PC può essere modificata dall'utente?	SI
Quale è la durata della password di rete?	In automatico 6 mesi
Lo USERID viene revocato in caso di mancato utilizzo?	SI, dopo sei mesi a partire dall'ultimo rinnovo password non eseguito
La password di rete ha una lunghezza minima?	SI, 8 caratteri o comunque il massimo numero di caratteri consentiti dal sistema di autenticazione utilizzato
Quanti sono i tentativi di prova di una password di rete prima che lo USERID sia disabilitato?	5
Com'è una password sicura?	Almeno 8 caratteri di cui una lettera maiuscola e un carattere speciale (es. ?, !, *, etc.). Le lettere non devono avere un senso compiuto (come nomi) non deve contenere né nome né cognome né parti di essi

Tabella 3 – Regole valide per userid e password per l'accesso alla rete

In generale, l'utilizzo della autenticazione tramite il server di dominio non esclude l'utilizzo della password BIOS.

Per quanto riguarda il salvataggio dei dati personali residenti sulle postazioni di lavoro **dell'Amministrazione Centrale**, a ciascun autorizzato è assegnato un codice identificativo personale e un PUK (Personal Unblocking Key) reperibile tramite AppIO seguendo le istruzioni disponibili all'indirizzo softwaresso.unina.it. Reperito il PUK si potrà impostare una password per i servizi di rete mediante i quali l'autorizzato può accedere ed utilizzare le risorse di rete. Ciascun autorizzato in possesso di credenziali di autenticazione alla rete ha accesso, in lettura e scrittura o come indicato dal responsabile dell'ufficio, ad uno spazio comune dedicato al proprio ufficio (Collabora) e, in lettura e scrittura, ad uno spazio personale (Onedrive); l'accesso potrà avvenire anche con sistemi di Multi-Factor Authentication. Tale spazio in cloud privato deve essere utilizzato per la conservazione ed elaborazione dei file di ufficio (Collabora) e può essere utilizzato per archiviare i file personali (Onedrive). Sul PC possono restare al termine del lavoro esclusivamente i file personali. Le cartelle cloud di Collabora risiedono su server gestiti dal CSI, in modo tale da garantire integrità, disponibilità e riservatezza dei dati registrati. L'accesso (in lettura, in scrittura, in lettura/scrittura) alle sotto-cartelle contenute nella cartella comune viene consentita agli incaricati afferenti all'intero Ufficio, oppure a gruppi nell'ambito dell'Ufficio, oppure a singoli dipendenti, sulla base di specifiche richieste concordate tra il Referente ed il CSI. In assenza di richieste, la regola base adottata dal CSI. è di consentire, per ciascunUfficio, l'accesso in lettura/scrittura a tutti gli autorizzati dell'Ufficio stesso.

Richieste di accessibilità ad ulteriori risorse di rete sono specificate ed autorizzate mediante il modulo SICURDAT/B.

Il referente è tenuto a verificare che siano rispettate le indicazioni precedentemente riportate da parte di ciascun autorizzato.

In nessun caso, per i PC collegati in rete, il salvataggio dei dati può essere effettuato su supporti di memorizzazione rimovibili (PENDRIVE-CHIAVETTA USB, CDROM, DVD) onde evitare esfiliazione di dati causato dalla perdita o sottrazione dei rimovibili

3.2.4 *Adempimenti specifici previsti per il caso c) – PC collegati in rete ed alle applicazioni centralizzate*

A tali PC si applicano le norme previste per il caso b), con l'aggiunta delle prescrizioni di seguito riportate.

Il referente del trattamento dei dati dovrà individuare, tassativamente per iscritto, compilando l'apposito modulo SICURDAT/B, gli autorizzati dei trattamenti informatizzati mediante procedure centralizzate. Tale designazione conferisce, implicitamente, anche l'autorizzazione all'utilizzo della corrispondente procedura informatica. I permessi dell'utente saranno tali da consentire le operazioni di trattamento richieste nel modello SICURDAT/B. I profili di abilitazione di ciascun autorizzato sono tenuti ed aggiornati dal CSI.

Di seguito, infine, si riportano alcune informazioni utili sulla gestione del codice identificativo personale (userid) e della password per l'accesso alle applicazioni informatiche centralizzate.

Ad ogni utente delle applicazioni informatiche centralizzate è associato un codice identificativo personale (userid), un PUK e una password ed un profilo di abilitazione. Alcune applicazioni prevedono due diversi livelli di identificazione: uno di *sistema* ed uno *applicativo*.

Qualsiasi applicazione che non rientra nell'elencazione del SICURDAT/B deve essere autorizzata dall'Ateneo per l'utilizzo del trattamento di dati personali (p.e. Form creati in qualsiasi modo per qualsiasi scopo o Test che richiedono iscrizione o Corsi online che richiedono iscrizione)

I codici di abilitazione disponibili per le diverse applicazioni sono riportati nel modello SICURDAT/B.

	SIRP	CSA	GEDAS	SIOC	GUTTEL	E-GRAMMATA	CIA	GTIK	VALCOM	BIBL. DIGIT. (Aleph)	CONCORSITA	TIROCINI	JOB LAUREATI
Livelli di identificazione	1	2	1	1	1	1	2	2	1	1	1	1	1
La password può essere modificata dall'utente?	SI	SI	SI	SI	SI	SI	SI	SI	NO	SI	NO	SI	SI
Quale è la durata della password ?	30 gg.	90 gg.	30 gg.		180 gg.		90 gg.	30 gg.	60gg.	90gg.			
Lo userid viene revocato in caso di mancato utilizzo?	NO	NO	NO	NO	NO	NO	NO	SI, dopo 45 gg.	NO	SI dopo 180 gg.	NO	NO	NO
La password ha una lunghezza minima?	NO	SI (8)	SI (6)	SI (3)	SI (8)	SI (8)	SI (8)	SI (6)	NO	SI (5)	SI (8)	SI (5)	SI (8)
Tentativi di prova della password prima che lo USERID sia disabilitato		5 userid sist.			3		5 userid sist.	5	3		10		

Tabella 4 – Regole valide per userid e password delle applicazioni informatiche centralizzate

3.2.5 *Utilizzo della rete Internet*

Il sistema informativo dell'Ateneo ed i dati in esso contenuti possono subire gravi danneggiamenti per effetto di un utilizzo improprio della connessione alla rete Internet; inoltre, attraverso tale rete possono penetrare nel sistema virus informatici ed utenti non autorizzati. Allo scopo di evitare questi pericoli, gli Autorizzati che dispongono di PC collegati in rete (caso b) e c)), curano l'applicazione delle seguenti regole:

1) utilizzano la connessione ad Internet esclusivamente per lo svolgimento dei compiti istituzionali dell'Ufficio;
2) si astengono da un uso di Internet illegale o non etico;
3) rispettano l'obbligo di non collegarsi a siti con materiale illegale e/o inappropriato;
4) si astengono dall'inviare, ricevere o mostrare testi o immagini che possono essere offensivi per le persone presenti;
5) rispettano i diritti di proprietà intellettuale facendo solo copie autorizzate di programmi o dati coperti da copyright;
6) non danneggiano né alterano il Setup o la configurazione software della propria postazione di lavoro, evitando inoltre di installare prodotti software non licenziati e/o non certificati a corredo della postazione per la specifica destinazione d'uso;
7) rispettano la privacy delle altre persone non facendosi passare per un altro utente della rete, non tentando di modificare o accedere a file, password o dati che appartengono ad altri, non cercando di disattivare il controllo di autorizzazione all'accesso a qualunque sistema o rete di computer;
8) non diffondono messaggi di posta elettronica di provenienza dubbia, non partecipano a sequenze di invii di messaggi (catene di S. Antonio) e non inoltrano o diffondono messaggi che annunciano nuovi virus;
9) sono referenti dell'uso della casella di posta elettronica istituzionale loro assegnata, non utilizzano le caselle di posta elettronica istituzionali per fini privati o personali, limitano allo stretto indispensabile l'invio di messaggi di posta elettronica con allegati, scegliendo, ove necessario, il formato degli allegati che occupa meno spazio;
10) non utilizzano servizi di comunicazione e condivisione files che esulino dalle ordinarie funzioni di browsing internet (https), posta elettronica e trasferimento files messi a disposizione dell'ateneo in area riservata (GigaMail, Office365, Collabora);
11) sono a conoscenza degli articoli del Codice Penale 615 ter – "*Accesso abusivo ad un sistema informatico o telematico*", 615 quater – "*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*", 615 quinquies – "*Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*", nonché del Decreto legge 22 marzo 2004 n.72 convertito in legge con modificazioni dalla Legge 21 maggio 2004 n.128, (Legge Urbani) che sanziona la condivisione e/o la fruizione di file relativi ad un'opera cinematografica o assimilata protetta dal diritto d'autore.

3.2.6 *Utilizzo di supporti rimovibili*

E' vietata la scrittura di categorie particolari di dati personali e dati personali relativi a condanne penali e reati (artt. 9 e 10 del Regolamento UE 2016/679) su supporti rimovibili (DVD, dispositivi USB, CDROM, CD riscrivibili, etc.). Qualora se ne ravvisi l'indispensabilità, è necessario la criptazione del supporto e ridurre al minimo la permanenza di tali dati sul dispositivo utilizzato e, al termine del trattamento effettuato, provvedere:

- alla loro cancellazione mediante tecniche che li rendano non intelligibili e ricostruibili, se riutilizzati per differenti trattamenti,
  oppure,
- alla loro distruzione,
  oppure,
- alla loro conservazione secondo quanto prescritto al successivo punto.

3.3 Trattamenti non automatizzati (cartacei)

L'autorizzazione al trattamento di dati personali, categorie particolari di dati personali e dati personali relativi a condanne penali e reati (artt. 9 e 10 del Regolamento UE 2016/679) effettuato senza l'ausilio di strumenti elettronici è richiesta dal referente mediante il modello SICURDAT/A.

L'allegato A**,** in aggiunta alle disposizioni di carattere generale valide per tutti i trattamenti non automatizzati di seguito riportate, contiene le "DISPOSIZIONI RELATIVE AL PROTOCOLLO E AGLI ARCHIVI", valide per le Strutture autonome e, soprattutto, per l'Amministrazione Centrale.

3.3.1 Dati personali non rientranti nelle categorie particolari né relativi a condanne penali e reati (art. 8 del Regolamento UE 2016/679)

I referenti del trattamento dei dati provvedono ad attuare le misure di protezione tese ad evitare l'accesso a persone non autorizzate ad archivi contenenti dati personali. Tra le misure utilizzabili si individuano le seguenti misure:

1) la sistemazione degli archivi e dei fascicoli in locali protetti da serrature;
2) l'utilizzo di mobili muniti di serrature per la raccolta e la conservazione dei fascicoli e dei documenti;
3) l'utilizzo di armadi ignifughi per la conservazione dei supporti informatici sui quali siano presenti copie di archivi contenenti dati personali.

Gli autorizzati del trattamento dei dati evitano comportamenti che possano pregiudicare la riservatezza dei dati. Per esigenze specifiche chiedono indicazioni e direttive al referente del trattamento dei dati.

3.3.2 Categorie particolari di dati personali e dati personali relativi a condanne penali e reati (artt. 9 e 10 del Regolamento UE 2016/679)

È obbligatorio conservare tali dati solo in contenitori appositamente individuati, evitando di lasciare le pratiche contenenti categorie particolari di dati personali sulla scrivania o comunque a portata di mano, se non per il tempo necessario all'effettivo utilizzo dei dati, al termine del quale le pratiche vanno comunque riposte.

Ogni autorizzato deve riporre i documenti o i supporti informatici contenenti categorie particolari di dati personali o dati personali relativi a condanne penali e reati negli appositi contenitori o scaffali al termine delle operazioni affidate e comunque a fine giornata. In ogni caso di allontanamento dal proprio posto di lavoro, i documenti devono essere riposti o negli armadi o nei cassetti e chiusi a chiave.

I dati idonei a rivelare lo stato di salute o la vita sessuale devono essere conservati separatamente dagli altri dati.

3.3.3 I PIN degli studenti

Fra i dati personali vanno annoverati i PIN (codice numerico di identificazione personale) degli studenti attraverso la cui conoscenza è possibile la registrazione degli esami (verbale elettronico)

E', pertanto opportuno che gli elenchi contenenti i PIN, forniti alle Segreterie studenti dal CSI, vengano utilizzati e conservati con tutte le cautele del caso che i referenti provvederanno ad individuare.

3.4 Videosorveglianza

Il Garante per la protezione dei dati personali, con le Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video – Versione 2.0 – Adottate il 29 gennaio 2020 ha impartito le direttive per la corretta gestione dei sistemi di videosorveglianza, recepite all'art. 25 "Videosorveglianza" del Regolamento di Ateneo. In accordo con quanto previsto dalle predette Linee guida, si ricorda che:

- la videosorveglianza deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, di quanto prescritto da altre disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi (ad esempio, le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela, nonché le norme riguardanti la tutela dei lavoratori, con particolare riferimento alla legge 300/1970, lo Statuto dei lavoratori e ss.mm.ii.);
- va escluso ogni uso superfluo di tali sistemi ed evitati eccessi e ridondanze;
- va evitata la rilevazione di dati in aree che non sono soggette a concreti pericoli, o per le quali non ricorre un'effettiva esigenza di deterrenza;
- gli scopi perseguiti devono essere tra quelli di pertinenza del titolare, cioè di protezione di specifiche aree soggette a rischio di intrusioni, di controllo di ambienti di notevole affollamento, nonché di prevenzione di atti di vandalismo e/o danneggiamento del patrimonio universitario.

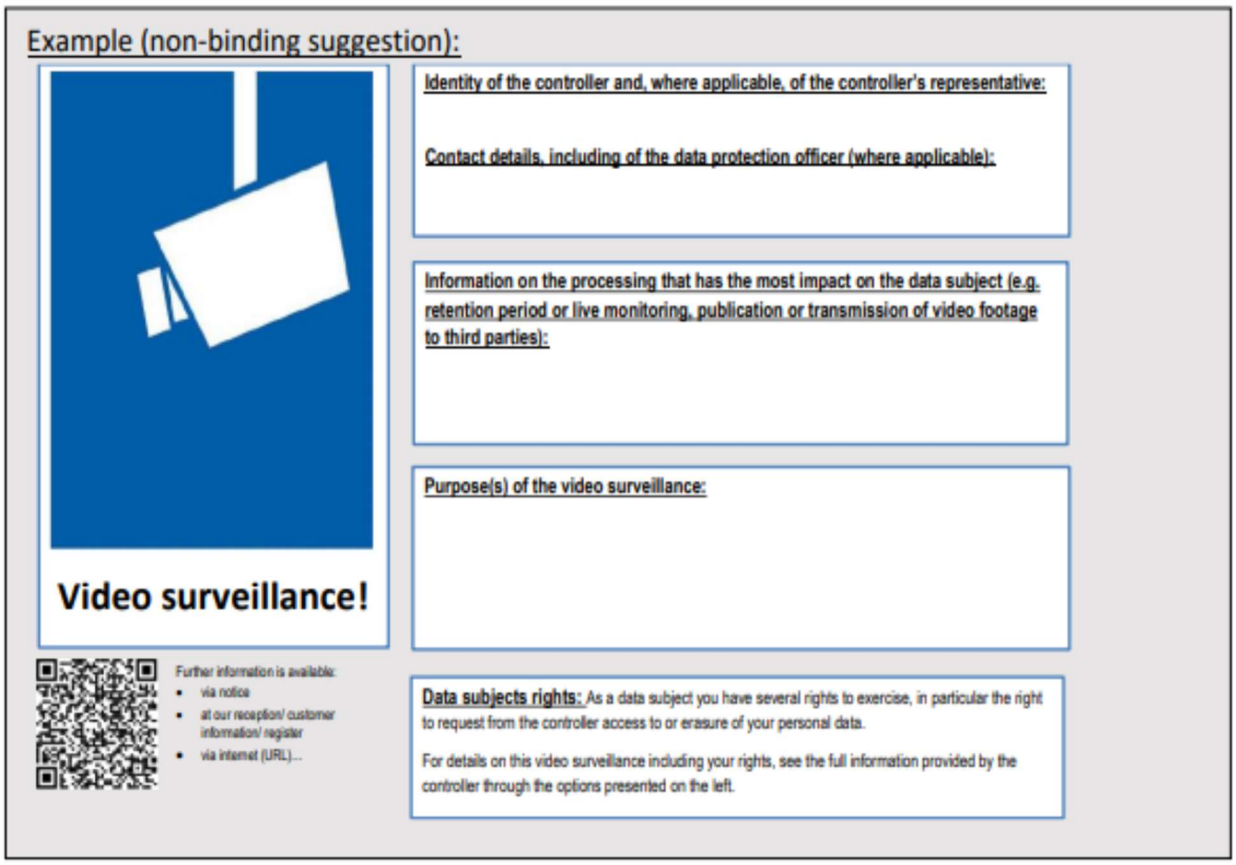
È opportuno ricordare che il referente dei trattamenti basati su sistemi di videosorveglianza di cui è titolare l'Università è nominato dall'Università tra il personale referente di uffici, strutture e servizi dell'Ateneo e provvede inoltre a designare gli autorizzati, individuandoli tra il personale afferente alla propria unità organizzativa. Se il servizio di videosorveglianza è erogato da una società esterna, questa è altresì nominata responsabile del trattamento contrattualmente affidatole e provvede a designare per iscritto i propri autorizzati, dandone comunicazione all'Università. Pertanto, se il servizio è erogato sia da personale dell'Università che da una società esterna, sono designati dal titolare due referenti, ciascuno per il propriospecifico ambito di competenza (ad esempio: turno, abilitazione a svolgere la registrazione dei dati, etc.) formalizzato nell'atto di nomina.

Ciò premesso, si riportano di seguito le disposizioni che ciascun referente e ciascun responsabile in caso di videosorveglianza devono osservare:

- garantire che le immagini riprese siano visualizzate soltanto dagli Autorizzati appositamente nominati, esclusivamente per finalità di tutela dei beni e delle persone che si trovano nelle Sedi sorvegliate.
- garantire, altresì, che le immagini ove siano registrate siano conservate per un periodo non superiore alle 24 ore e che la visualizzazione delle immagini registrate avvenga esclusivamente nel caso in cui si verifichi un illecito o in relazione ad indagini dell'autorità giudiziaria o di polizia;
- garantire il diritto di accesso all'interessato. L'art. 6 "Diritti dell'interessato" delle precitate Linee guida 3/2019 prevede che: "Un interessato ha diritto di ottenere dal titolare del trattamento la conferma o meno del fatto che i propri dati personali siano oggetto di trattamento. Per quanto riguarda la videosorveglianza, ciò significa che se nessun dato è conservato o trasferito, una volta trascorso il momento del monitoraggio in tempo reale, il titolare potrebbe soltanto comunicare che nessun dato personale è più oggetto di trattamento (oltre alle informazioni generali obbligatorie di cui all'articolo 13, si veda la sezione 7 – Obblighi di trasparenza e informazione). Se tuttavia i dati sono ancora in corso di trattamento al momento della richiesta (vale a dire se i dati sono conservati o trattati ininterrottamente in qualsiasi altro modo), l'interessato dovrebbe ricevere accesso e informazioni

conformemente alle disposizioni dell'articolo 15";

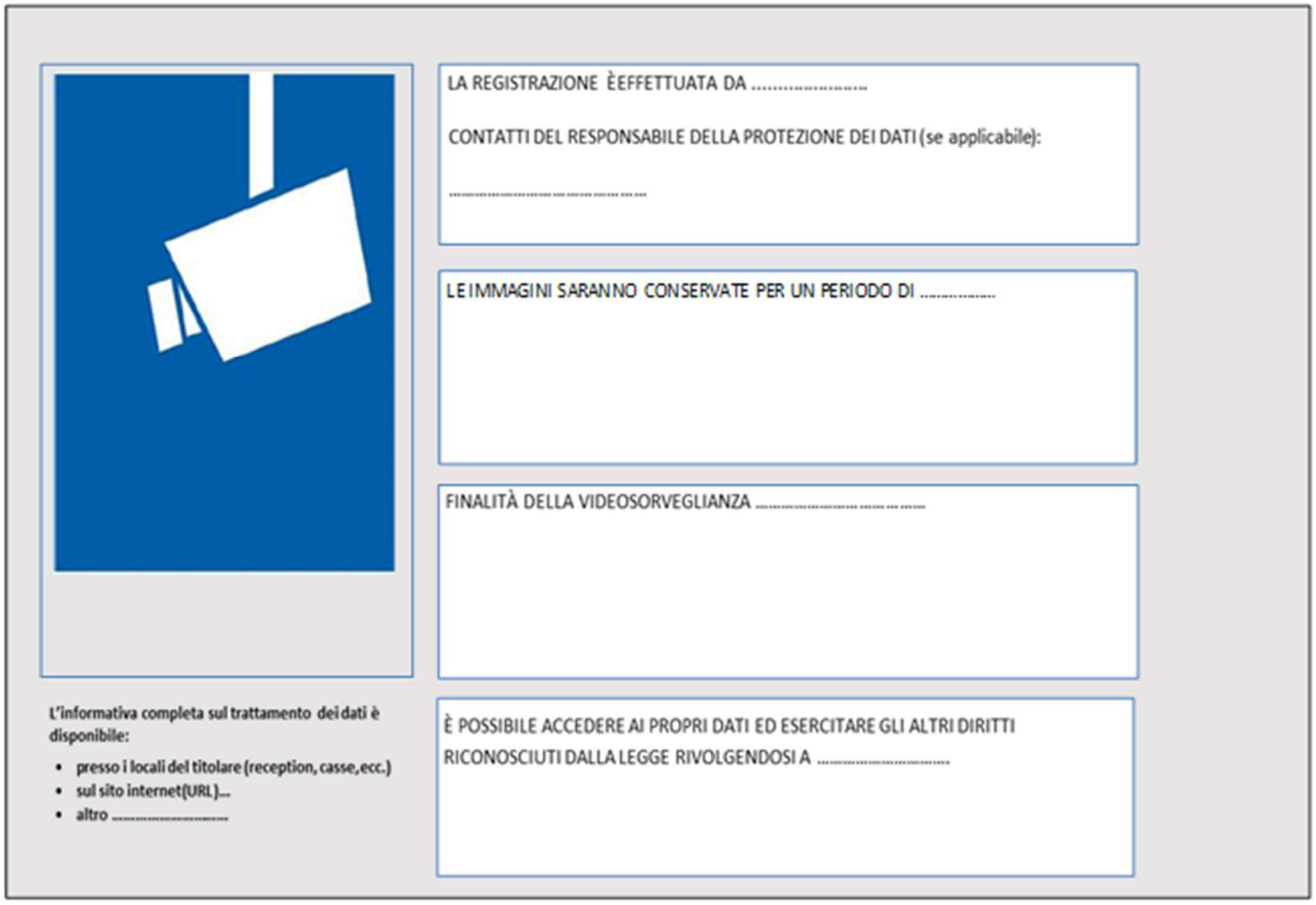
- rendere inoltre alle persone che possono essere riprese idonea informativa, ai sensi dell'art. 13 del Regolamento UE 2017/679, circa la presenza degli impianti, curandosi di affiggere appositi cartelli nei luoghi ripresi dalle telecamere. In particolare, potrà utilizzare in aree esterne il modello semplificato di informativa "minima" elaborato dal Garante per la Protezione dei Dati Personali, di seguito riportato in fac-simile.



MODELLO SEMPLIFICATO CARTELLO VIDEOSORVEGLIANZA

(EDPB - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - adottate il 29 gennaio 2020)

Per informazioni: www.garanteprivacy.it/faq/videosorveglianza



Schema del testo dell'informativa da riportare sui cartelli esposti:

Nel primo riquadro del cartello, alla voce: "La Registrazione è effettuata da…", si deve il Titolare del trattamento: Università degli Studi di Napoli Federico II – Dipartimento di/Centro (inserire denominazione)[1].
Il secondo riquadro deve indicare se il sistema prevede la registrazione delle immagini o la semplice visualizzazione delle stesse (in tempo reale). Nel caso di registrazione si devono riportare le informazioni relative al periodo di conservazione delle immagini acquisite e se tali informazioni siano trasmesse a soggetti terzi (società nominate Responsabili dei trattamenti).
Il terzo riquadro deve elencare quali sono le specifiche finalità del trattamento.
Il quarto riquadro deve contenere le informazioni sulle modalità di esercizio dei diritti dell'interessato ai sensi degli artt. da 15 a 22, 77 e 79 del Regolamento UE 2016/679. Nel detto riquadro vanno riportati i dati di contatto della struttura di riferimento[2] e i dati di contatto del Responsabile della protezione dei dati (RPD): rpd@unina.it.

La cartellonistica (segnaletica di avvertimento di primo livello) deve contenere un chiaro riferimento a informazioni per esteso (informazioni di secondo livello) ad esempio attraverso un codice QR con l'indicazione di un indirizzo web alla pagina informativa completa, contenente tutti gli elementi di cui all'art. 13 del Regolamento UE 2016/679 ed indicando dov'è reperibile (ad es. sul sito Internet del titolare del trattamento o affisso in bacheche o locali dello stesso). Le dette informazioni in tema di videosorveglianza sono disponibili sul sito di Ateneo:
http://www.unina.it/documents/11958/25109316/Informazioni_trattamento_dati_videosorveglianza_2021-09-30.pdf.

[1] Il richiamo alla società esterna vale solo nel caso in cui ci sia un affidamento del servizio. Se tale affidamento è parziale, il riferimento alla società esterna segue quello del Referente e degli Autorizzati dell'Università; se l'affidamento è completo, allora si omette il riferimento iniziale al Referente e agli Autorizzati dell'Università e si riporta solo quello alla società di vigilanza.
[2] Inserire la denominazione ed un recapito telefonico dell'ufficio/struttura deputata a dare riscontro ad eventuali richieste dell'interessato.

4. RACCOMANDAZIONI GENERALI

4.1 Distanza di cortesia

L'udienza degli utenti va organizzata in modo da evitare che altri, dipendenti o non dipendenti,possano, anche involontariamente, ascoltare i colloqui che ciascun utente intrattiene con il personale addettoa recepire le relative istanze. Deve, cioè, essere garantita la *c.d. distanza di cortesia* nelle ipotesi in cui vengano in rilievo dati personali dell'interessato.

4.2 Linee guida per il corretto utilizzo di userid e password

La sicurezza logica si realizza assicurando che tutti gli accessi ai diversi componenti del sistema informativo dell'Ateneo avvengano esclusivamente secondo modalità prestabilite. Per tale motivo, ogni qual volta si rende necessario l'utilizzo di una risorsa informatica, deve essere presente un meccanismo che costringa l'utente (referente o autorizzato privacy) ad autenticarsi, ossia a dimostrare la propria identità, mediante tipicamente l'utilizzo di un codice identificativo personale (userid) ed una parola chiave (password).

Tutti gli utenti rispettano le seguenti disposizioni:

A) L'utente è referente della corretta tenuta della password di accensione del PC che gli è stato assegnato e delle eventuali password di accesso alla rete e alle applicazioni;
B) L'utente a cui è stata assegnata una userid per l'accesso alla rete e/o per l'utilizzo di applicazioni informatiche centralizzate, è referente di tutto quanto accade a seguito di transazioni ed elaborazioni abilitate dal proprio codice identificativo personale. Per le applicazioni informatiche centralizzate, tale responsabilità deve essere riferita ai privilegi associati al suo profilo di abilitazione;
C) L'utente cambia le proprie password secondo le disposizioni riportate nel presente manuale e comunque minimo ogni 6 mesi;
D) L'utente gestisce le proprie password secondo le disposizioni riportate nel presente manuale;
E) L'utente attiva tutte le misure in suo potere per evitare che terzi abbiano accesso al suo PC mentre si allontana durante una sessione di lavoro. A tal fine esce sempre dall'applicazione in uso (logoff) o eventualmente blocca il PC con uno screen saver protetto da password;
F) L'utente non comunica a nessun altro utente le proprie password.

In generale, vi sono diverse categorie di password, ognuna con il proprio ruolo preciso:

a) **la password di accensione del PC** (password di BIOS e locale) impedisce l'utilizzo improprio della propria postazione di lavoro, quando per un qualsiasi motivo non ci si trova in ufficio;
b) **la password di rete** impedisce che l'eventuale accesso non autorizzato ad un PC renda disponibili le risorse dell'ufficio (stampanti, cartelle condivise);
c) **la password delle applicazioni informatiche centralizzate** permette di restringere l'accesso alle funzioni e ai dati al solo personale autorizzato;

d) **la password del salva schermo** impedisce che un'assenza momentanea permetta a una persona non autorizzata di visualizzare il lavoro in corso e/o di accedere ai documenti residenti sulla postazione di lavoro.

La gestione delle password indicate sono disciplinate dal **Disciplinare tecnico in materia di misure minime di sicurezza - Allegato B** (regole da 1 a 11): in sintesi, esse hanno una lunghezza non inferiore ad 8 caratteri, oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo; queste password sono modificate dall' Autorizzato al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di categorie particolari di dati personali e di dati personali relativi a condanne penali e reati (artt. 9 e 10 del Regolamento UE 2016/679), la password deve essere modificata almeno ogni tre mesi. Le credenziali sono inoltre disattivate dopo sei mesi di mancato utilizzo e sono revocate nel caso di perdita delle qualità che consente all'utente l'accesso ai dati personali.

Le password di cui ai punti e) ed f) rappresentano un ulteriore livello di protezione il cui impiego è lasciato alla discrezione dell'utente della postazione di lavoro.

Nella gestione delle password è necessario attenersi alle indicazioni di seguito riportate.

Cosa NON fare:

1) NON comunicare a NESSUNO le proprie password, qualunque sia il mezzo che viene utilizzato per inoltrare la richiesta (telefono, messaggio di posta elettronica, ecc.). Ricordare che NESSUNO è autorizzato a richiedere le password, nemmeno il personale tecnico di supporto o gli addetti alla manutenzione delle postazioni di lavoro, e che lo scopo principale per cui sono utilizzate le password è di assicurare che nessun altro possa utilizzare le risorse a cui si è abilitati;
2) NON scrivere le password su supporti che possano essere trovati facilmente e/o soprattutto in prossimità della postazione di lavoro utilizzata;
3) NON scegliere password corrispondenti a parole presenti in un dizionario, sia della lingua italiana che di lingue straniere. Esistono programmi che permettono di provare come password tutte quelle contenute in dizionari elettronici estremamente ampi, in termini di numero di lemmi, e in diverse lingue, scritte sia in senso normale che in senso inverso;
4) NON usare come password il nome utente o parole che possano essere facilmente riconducibili all'identità dell'utente, come, ad esempio, il codice fiscale, il nome del coniuge, il nome dei figli, la data di nascita, il numero di telefono, la targa della propria auto, il nome della strada in cui si abita, il nome della squadra di calcio per cui si tifa, ecc.;
5) NON usare come password parole ottenute da una combinazione di tasti vicini sulla tastiera o sequenze di caratteri (esempio: qwerty, asdfgh, 123321, aaabbb, ecc.);
6) NON usare la STESSA password per le diverse tipologie di password prima individuate;
7) NON rendere note password vecchie e non più in uso, in quanto da questi dati è possibile ricavare informazioni su ciclicità e/o regole empiriche e personali che l'utente utilizza per generare le proprie password.

Cosa FARE:

1) Cambiare le password frequentemente ricordando che il limite massimo di validità di una password stabilito dalle presenti misure minime è di 6 mesi;
2) Utilizzare password lunghe almeno otto caratteri con un misto di lettere, numeri e segni di interpunzione e una lettera maiuscola;

3) Nella digitazione delle password assicurarsi che non ci sia nessuno che osservi ciò che si digita sulla tastiera del PC;
4) Utilizzare password distinte per le diverse tipologie di password prima descritte.

4.3 Come scegliere le password

La scelta della password da parte dell'utente deve essere oculata, in quanto il modo più semplice e più utilizzato per realizzare un accesso illecito ad un sistema e/o ad un'applicazione, consiste nell'ottenere le credenziali identificative di un utente autorizzato, ossia la sua coppia userid e password. La scelta, quindi, di password "forti" rappresenta un aspetto essenziale della sicurezza informatica.

Le password migliori sono quelle facili da ricordare ma, allo stesso tempo, difficili da individuare. Questo genere di password può essere ottenuto, ad esempio, comprimendo frasi lunghe in pochi caratteri presenti nella frase, utilizzando anche segni di interpunzione e caratteri maiuscoli e minuscoli. La frase "Nel 1969 l'uomo è andato sulla luna" può, ad esempio, fornire tra le tante possibilità la seguente "N69UèAsL".

Accanto a questa tecnica, per ottenere password ancora più "forti", si possono sostituire le lettere risultanti dalla compressione della frase, con cifre o caratteri che assomiglino alle lettere; ad esempio la frase "Questo può essere un modo per ricordare la password" diventa "Qp&1mpRP".

Un altro modo per ottenere password "forti" consiste nel combinare date o numeri che si ricordano facilmente con pezzi di parole che sono in qualche modo abituali e quindi semplici da ricordare; ad esempio la combinazione "felice1983", che utilizzata direttamente potrebbe essere una password "debole" (combinazione del nome del figlio e della data di nascita), può diventare una password migliore in questo modo "FeLi83ce", o una password "forte" così "F&Li83cE".

N.B. Non utilizzare come password gli esempi riportati nel presente manuale.

Allegato A - DISPOSIZIONI RELATIVE AL PROTOCOLLO ED AGLI ARCHIVI

A.1 Il Protocollo

Il protocollo rappresenta, ai fini della tutela della riservatezza, della disponibilità e della integrità, un settore particolarmente delicato, considerato che vi transitano tutti i documenti dell'Ateneo sia in entrata che in uscita. Ciò implica che gli addetti agli Uffici Protocollo di ciascuna struttura (Unità Organizzativa Referente) dell'Ateneo, anche se per il solo transito di documenti, gestiscono quasi la totalità delle informazioni che vengono trattate dall'amministrazione.

Risulta dunque indispensabile che essi siano particolarmente attenti, nello svolgimento delle attività di competenza, alla problematica in oggetto.

Si ribadiscono pertanto tutte le disposizioni dettate in precedenza per il trattamento dei dati personali (sia automatizzati che non automatizzati), sottolineando alcuni aspetti ulteriori che per il settore in argomento assumono particolare rilievo:

- l'accesso all'ufficio va costantemente controllato;
- gli addetti di altre strutture devono effettuare le operazioni di prelievo e consegna di documenti nel locale d'ingresso;
- non è consentito intrattenersi presso i locali dell'ufficio se non per il tempo strettamente necessario alla consegna o al prelievo;
- l'ufficio disporrà affinché una unità di personale sia addetta al ricevimento dei documenti, evitando l'accesso all'ufficio da parte di personale di altre strutture, quando ciò non sia necessario;
- ciascun addetto al protocollo deve avere accesso ai soli documenti indispensabili allo svolgimento dei compiti assegnati.

A.2 La tenuta dell'Archivio presso l'Amministrazione Centrale

Ad integrazione e parziale modifica del precedente Ordine di Servizio n. 47 del 31.01.2006, con Ordine di Servizio n. 403 del 7 dicembre 2007, si è provveduto a fornire ulteriori indicazioni in tema di sicurezza dei locali appositamente destinati all'archivio corrente del palazzo degli Uffici.

In particolare, la custodia delle chiavi dell'archivio è stata affidata ad una unità di personale afferente all'Ufficio Servizi Generali. La predetta unità di personale tiene, altresì, il registro degli accessi sul quale devono essere annotate le seguenti informazioni: l'ora di ingresso all'archivio e quella di uscita, il nominativo della persona che accede a locali e la tipologia di attività. Sono inoltre individuate in modo puntuale i nominativi dei sostituti (addetti alla custodia del Palazzo degli Uffici) che garantiscono l'accesso all'archivio nelle ore successive all'orario di servizio dell'autorizzato.

A.3 La tenuta dell'Archivio presso le Strutture autonome

Presso ciascuna Struttura autonoma sono individuati dei locali chiusi a chiave per l'archiviazione dei documenti edei fascicoli. La custodia ed il controllo sul prelievo e ricollocazione della documentazione di volta in volta occorrente agli uffici della Struttura autonoma è formalmente affidata, dal Direttore, ad un ufficio della Struttura autonoma.

Il personale addetto al controllo dell'archivio dovrà consentire l'accesso all'archivio esclusivamente al personale munito di autorizzazione firmata dal referente dell'ufficio richiedente ed opportunamente esibita. Tale autorizzazione sarà debitamente firmata dall'autorizzato dell'ufficio richiedente, per ricevuta. La consegna della documentazione sarà, in modo del tutto analogo, accompagnata da una nota firmata dall'ufficio richiedente e controfirmata, per accettazione, da parte dell'ufficio preposto alla tenuta dell'archivio.

Allegato B - ACCORGIMENTI PER GLI AMMINISTRATORI DI SISTEMA

Gli Amministratori di Sistema (AdS), designati in virtù del Provvedimento a carattere generale del Garante per la Protezione dei Dati Personali del 27.11.2008 titolato "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", oltre a garantire il rispetto delle prescrizioni fornite dal Titolare precedentemente illustrate, devono inoltre garantire, sulla base del proprio profilo di AdS, il rispetto delle misure minime di sicurezza di seguito elencate:

Profilo AdS-Sistema

- assicurare la gestione ed il corretto funzionamento dei sistemi di autenticazione ed autorizzazione degli utenti sui sistemi server in uso;
- eseguire la verifica periodica, ogni 6 mesi, degli utenti autorizzati sui sistemi server in uso provvedendo alla cancellazione degli utenti non più in possesso dell'autorizzazione all'accesso:
- predisporre e rendere funzionanti le copie di sicurezza (backup e recovery) dei sistemi server in uso;
- predisporre sistemi idonei alla registrazione degli accessi logici ai sistemi server in uso. Tali registrazioni devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste;
- predisporre sugli elaboratori del sistema informativo i meccanismi per la protezione dei sistemi contro il rischio di intrusione ad opera di programmi di cui all'art. 615 quinquies del codice penale, mediante idonei programmi la cui efficacia ed aggiornamento siano verificati con cadenza almeno semestrale;
- predisporre ed aggiornare i programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti, con cadenza almeno semestrale;
- adottare ulteriori misure di sicurezza previste dal Regolamento UE 2016/679 per i trattamenti di categorie particolari di dati personalio e di dati personali relativi a condanne penali e reati, finalizzate alla protezione dei dati contro l'accesso abusivo, alla custodia o alla distruzione dei supporti rimovibili su cui sono memorizzati i dati, al ripristino dell'accesso aidati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi compatibili con i diritti degli interessati e non superiori a sette giorni.

Profilo AdS-Database

- assicurare la gestione ed il corretto funzionamento dei sistemi di autenticazione ed autorizzazione degli utenti sui database in uso;
- eseguire la verifica periodica, ogni 6 mesi, degli utenti autorizzati sui database in uso provvedendo alla cancellazione degli utenti non più in possesso dell'autorizzazione all'accesso:
- predisporre e rendere funzionanti le copie di sicurezza (backup e recovery) dei database in uso;
- predisporre sistemi idonei alla registrazione degli accessi logici ai database in uso. Tali registrazioni devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
- predisporre ed aggiornare i programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti, con cadenza almeno semestrale;

- adottare ulteriori misure di sicurezza previste dal Regolamento UE 2016/679 per i trattamenti di categorie particolari di dati personali o di dati personali relativi a condanne penali e reati, finalizzate alla protezione dei dati contro l'accesso abusivo, alla custodia o alla distruzione dei supporti rimovibili su cui sono memorizzati i dati, al ripristino dell'accesso aidati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi compatibili con i diritti degli interessati e non superiori a sette giorni.

Profilo AdS-Rete

- assicurare la gestione ed il corretto funzionamento degli apparati di accesso e di distribuzione per la rete di Ateneo con particolare riferimento ai relativi sistemi di autenticazione e autorizzazione atti a proteggere gli accessi per le attività di amministrazione, gestione e configurazione degli stessi;
- eseguire la verifica periodica, ogni 6 mesi, degli utenti (AdS) autorizzati all'accesso (necessario per le sole attività di amministrazione) agli apparati di rete provvedendo alla cancellazione degli utenti non più in possesso dell'autorizzazione all'accesso;
- predisporre sistemi idonei alla registrazione degli accessi logici agli apparati di rete in esercizio. Tali registrazioni devono avere caratteristiche di completezza, in alterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Profilo AdS-Applicazione

- assicurare la gestione ed il corretto funzionamento dei sistemi di autenticazione ed autorizzazione degli utenti sulle applicazioni in uso;
- eseguire la verifica periodica, ogni 6 mesi, degli utenti autorizzati sulle applicazioni in uso provvedendo alla cancellazione degli utenti non più in possesso dell'autorizzazione all'accesso;
- predisporre ed aggiornare i programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti, con cadenza almeno semestrale.