UNIVERSITÀ DI PISA
DIREZIONE AFFARI LEGALI E GENERALI
Dirigente ad interim: Dottor Riccardo Grasso
Sostituto del Dirigente: Avv. Sandra Bernardini
Unità Elettorale, Normativa e Costituzione Strutture Universitarie/AS/sb

IL RETTORE

VISTA: la Legge 9 maggio 1989, n. 168, in particolare l'articolo 6, comma 1, "Autonomia delle Università";

VISTA: la Legge 30 dicembre 2010, n. 240 - "Norme in materia di organizzazione delle università, di personale accademico e di reclutamento, nonché delega al Governo per incentivare la qualità e l'efficienza del sistema universitario" e successive modifiche, in particolare l'articolo 6, commi 7 e 8;

VISTO: lo Statuto di Ateneo, emanato con decreto rettorale 27 febbraio 2012, n. 2711 e successive modifiche;

VISTO: il Regolamento di Ateneo per la tutela delle persone e di altri soggetti rispetto al trattamento di dati personali, emanato con Decreto Rettorale 7 ottobre 1998, n. 1422, e successive modifiche;

VISTO: il Regolamento dell'Unione Europea (UE), n. 679/2016, "Regolamento generale sulla protezione dei dati, finalizzato ad assicurare un'applicazione della disciplina della privacy omogenea su tutto il territorio dell'Unione Europea";

VISTO: il Decreto Legislativo n. 196/2003, e successive modifiche, come da ultimo novellato dal Decreto Legislativo n. 101/2018 "Codice in materia di protezione dei dati personali";

VISTA: la bozza di regolamento in materia di protezione dei dati personali in attuazione del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio e del Decreto Legislativo 30 giugno 2016, n. 196, "Codice in materia di protezione dei dati personali", elaborata dalla CRUI – Conferenza dei Rettori delle Università Italiane;

RILEVATA: la necessità di approvare un nuovo regolamento in materia di protezione dei dati personali all'interno dell'Università di Pisa, al fine di adeguare la regolamentazione alle importanti novità introdotte dalla normativa europea e recepite dall'ordinamento nazionale;

VISTA: la delibera del 19 aprile 2019, n. 119, con la quale il Consiglio di Amministrazione ha espresso parere favorevole alla proposta di regolamento per la protezione dei dati personali dell'Università di Pisa;

VISTA: la delibera del 17 maggio 2019, n. 113, con la quale il Senato Accademico ha approvato la predetta proposta di regolamento;

DECRETA

Articolo 1

1. E' emanato il Regolamento per la protezione dei dati personali dell'Università di Pisa, allegato al presente decreto di cui è parte integrante.

Articolo 2

1. Il presente decreto entra in vigore il quindicesimo giorno successivo alla sua pubblicazione nell'Albo Ufficiale Informatico di Ateneo. Il regolamento è inoltre consultabile sul sito dell'Ateneo.

Il Rettore
Paolo M. Mancarella

Regolamento per la protezione dei dati personali nell'Università di Pisa

Titolo I
Premesse e norme definitorie

Articolo 1 - Ambito di applicazione

1. Il presente regolamento disciplina il trattamento dei dati personali all'interno dell'Università di Pisa (di seguito Università), ai sensi del regolamento dell'Unione Europea (UE) n. 679/2016 "Regolamento generale sulla protezione dei dati", del decreto legislativo 30 giugno 2003, n.196, "Codice in materia di protezione dei dati personali", come novellato dal decreto legislativo 10 agosto 2018, n.101, e della normativa vigente.
2. L'Università procede al trattamento, alla comunicazione e alla diffusione di dati personali nell'ambito del perseguimento dei propri fini istituzionali, nei limiti stabiliti dalla legge, dallo statuto e dai regolamenti di Ateneo.
3 Lo scopo del presente regolamento è quello di garantire che le procedure per il trattamento dei dati personali dell'Ateneo siano effettuate nel rispetto dei diritti, delle libertà fondamentali, della dignità delle persone, avuto particolare riguardo alla riservatezza e all'identità personale degli utenti, interni ed esterni e, più in generale, di tutti coloro i quali abbiano rapporti con l'Ateneo.

Articolo 2 – Definizioni

1. Ai fini del presente regolamento, si intende per
   - dato personale: qualunque 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 online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
   - categorie particolari di dati: i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, i dati genetici, i dati biometrici atti a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale;
   - dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica;
   - dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
   - dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione a suo favore di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
   - trattamento dei dati: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di 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, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- limitazione di trattamento: il contrassegno temporale dei dati personali conservati con l'obiettivo di limitarne il trattamento nel tempo;
- profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti;
- pseudonimizzazione: il trattamento dei dati personali in modo tale che gli stessi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative volte a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, autonomamente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- designato al trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- responsabile per la protezione dei dati: la persona fisica specializzata nel supporto al titolare del trattamento, prevista come obbligatoria negli enti pubblici (di seguito RPD);
- autorizzati al trattamento: le persone fisiche formalmente autorizzate e istruite a trattare i dati personali sotto l'autorità diretta del titolare e/o designato e per le finalità stabilite dal titolare;
- destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi;
- terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il designato, il responsabile del trattamento e la persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- interessato al trattamento: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, a che i dati personali che lo riguardano siano oggetto di trattamento;
- responsabile della transizione al digitale: figura i cui compiti sono definiti dall'articolo 17, comma 1-sexies del codice dell'amministrazione digitale[1].
- responsabile della conservazione dei documenti informatici: figura i cui compiti sono definiti dall'articolo 44 del codice dell'amministrazione digitale[1];
- responsabile della sicurezza informatica: figura i cui compiti saranno definiti da apposito regolamento;
- referente di struttura per la sicurezza: persona fisica individuata da ciascun dipartimento, direzione o altra struttura prevista nel modello organizzativo cui è affidato il compito della

[1] Emanato con decreto legislativo 7 marzo 2005 n.82, quale risultante dalle successive modifiche e integrazioni, inclusa l'ultima disposizione integrativa e correttiva di cui al decreto legislativo 13 dicembre 2017, n.217 "Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche"

gestione locale dei sistemi e della rete nel rispetto delle norme stabilite dalla normativa vigente in materia;
- violazione dei dati personali: violazione di sicurezza che comporta accidentalmente o volontariamente la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- autorità di controllo: Autorità garante per la protezione dei dati personali;
- trattamento transfrontaliero: trattamento di dati personali che ha luogo nell'ambito dell'attività di stabilimenti in più di uno Stato membro ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno stato membro; trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno stato membro;
- stabilimento principale: luogo in cui il titolare del trattamento nell'Unione europea ha la sua sede legale. Quando le decisioni sulle finalità e sui mezzi del trattamento sono adottate in un altro stabilimento, quest'ultimo viene considerato lo stabilimento principale.

Titolo II
Principi e modalità del trattamento

Articolo 3 - Principi applicabili al trattamento di dati personali

1. Il trattamento dei dati personali deve avvenire nel rispetto dei seguenti principi:
   a) liceità, correttezza e trasparenza;
   b) limitazione delle finalità che devono essere determinate, esplicite e legittime; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a scopi statistici non è considerato incompatibile con le finalità iniziali;
   c) adeguatezza, pertinenza e limitazione a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);
   d) esattezza e, se necessario, aggiornamento; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
   e) limitazione della conservazione per il tempo necessario al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;
   f) integrità e riservatezza, in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante l'adozione di misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.
2. Il titolare del trattamento è competente per il rispetto di tutti i principi disciplinati dal regolamento europeo e deve essere in grado di comprovarlo secondo il principio di responsabilizzazione (accountability).

Articolo 4 - Base giuridica del trattamento

1. L'Università è una pubblica amministrazione ai sensi dell'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n.165 e successive modifiche, persegue finalità di interesse generale, opera in regime di diritto pubblico ed esercita potestà pubbliche. Pertanto, il trattamento di dati personali nell'esercizio dei propri compiti istituzionali trova il fondamento di liceità nella condizione prevista dall'articolo 6, comma 1, del regolamento europeo.
2. Il trattamento deve sempre essere necessario al perseguimento dei fini per i quali viene lecitamente effettuato (principio di necessità).

Articolo 5 - Trattamento di categorie particolari di dati personali

1. È vietato trattare dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
2. Il trattamento dei dati personali di cui al comma 1 non è vietato quando:
   a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
   b) è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
   c) è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
   d) il trattamento è effettuato, nell'ambito di attività autorizzate e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, attuali o precedenti, o le persone che interagiscono lecitamente con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
   e) riguarda dati personali resi manifestamente pubblici dall'interessato;
   f) è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
   g) è necessario per motivi di interesse pubblico, è proporzionato alla finalità perseguita, prevede misure appropriate e specifiche per tutelare i diritti fondamentali dell'interessato;
   h) è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali ed è eseguito sotto la responsabilità di un professionista soggetto al segreto professionale;
   i) è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici;
   j) è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali dell'interessato.

Articolo 6 - Trattamento di dati personali relativi a condanne penali e reati

1. Il trattamento di dati personali relativi a condanne in sede penale, a reati e a connesse pene e misure di sicurezza, è consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, ai sensi dell'articolo 2-octies del codice in materia di protezione dei dati personali.

Titolo III
I soggetti

Articolo 7 - Titolare del trattamento

1. L'Università, nella persona del Rettore, legale rappresentante pro tempore, è titolare del trattamento dei dati personali.
2. Mette in atto le misure tecniche e organizzative adeguate a garantire che il trattamento sia effettuato in conformità alla vigente normativa europea, nazionale e di Ateneo, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Articolo 8 - Contitolare

1. Quando uno o più titolari del trattamento determinano congiuntamente all'Università le finalità e i mezzi del trattamento, essi sono contitolari del trattamento.
2. L'Università e il contitolare del trattamento determinano in modo trasparente, mediante un accordo, i rispettivi obblighi in merito all'osservanza del regolamento europeo, con particolare riguardo all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni richieste dall'informativa privacy, salvo che i predetti obblighi e funzioni siano già disciplinati da espresse previsioni di legge.
3. L'accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
4. L'interessato può esercitare i propri diritti nei confronti di ciascun contitolare del trattamento.

Articolo 9 - Responsabile della protezione dei dati personali - RPD

1. Il RPD è individuato e designato dal titolare tra il personale docente o tecnico amministrativo dell'Università di Pisa in funzione delle qualità professionali e, in particolare, della conoscenza specialistica della normativa in materia di protezione dei dati personali e della legislazione universitaria.
2. Il RPD in particolare:
    a) informa e fornisce consulenza al titolare del trattamento, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal presente regolamento, dalla normativa europea e nazionale inerenti alla protezione dei dati;
    b) vigila sull'osservanza del presente regolamento e di altre disposizioni previste dalla normativa europea e nazionale, ivi comprese le politiche del titolare in materia di protezione dei dati personali fra le quali l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
    c) fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorveglia lo svolgimento;
    d) coopera con il Garante per la protezione dei dati personali;
    e) funge da tramite con il Garante per la protezione dei dati personali in ordine a questioni connesse al trattamento, tra cui la consultazione preventiva, quando la valutazione di impatto indichi un rischio elevato correlato al trattamento stesso;
    f) collabora con i designati nella redazione e aggiornamento dei registri di trattamento di cui all'articolo 29 del presente regolamento.
3. Nell'eseguire i propri compiti il RPD considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
4. Al RPD sono garantiti supporto, risorse e tempi di lavoro adeguati allo svolgimento della sua funzione. Al RPD è garantita, inoltre, una formazione permanente che gli assicuri l'aggiornamento costante sugli sviluppi nel settore della protezione dei dati.
5. Il RPD ha ampio accesso alle informazioni ed è interpellato su ogni problematica inerente alla protezione dei dati e in merito ad ogni attività che, a partire dalla sua progettazione, implica un trattamento dati.
6. L'Università garantisce che il RPD eserciti le proprie funzioni in autonomia e indipendenza e assegna allo stesso esclusivamente attività o compiti che non risultino in contrasto o in conflitto di interesse.
7. Il RPD non riceve alcuna istruzione per quanto riguarda l'esecuzione dei compiti a lui affidati.
8. L'Università non rimuove o penalizza il RPD in ragione delle modalità dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni.

9. Il nominativo e i dati di contatto del RPD sono comunicati al Garante per la protezione dei dati personali. I dati di contatto del RPD sono inseriti nelle informative privacy e pubblicati sul sito internet istituzionale.
10. Su indicazione del RPD possono essere costituiti specifici gruppi di lavoro in materia di adeguamento alla normativa sulla protezione dei dati personali.

Articolo 10 – Designati al trattamento

1. I designati al trattamento dei dati personali sono così individuati:
   a) per le strutture amministrative centrali dell'Ateneo: il Direttore generale e i dirigenti per le rispettive attività di competenza;
   b) per le strutture didattiche, di ricerca e di servizio: i direttori dei dipartimenti e dei centri di Ateneo con autonomia gestionale e amministrativa, i presidenti dei sistemi di Ateneo.
2. I designati sono tenuti:
   a) a trattare i dati personali secondo quanto stabilito dal presente regolamento;
   b) a garantire e vigilare che le persone autorizzate rispettino il segreto d'ufficio e la normativa in materia di protezione dei dati personali;
   c) ad assistere il titolare del trattamento nel garantire il rispetto degli obblighi di legge in materia di protezione dei dati, in base alla natura del trattamento e delle informazioni a loro disposizione;
   d) a svolgere con diligenza e perizia tutte le attività ad essi assegnate dalla normativa vigente[2];
   e) a consentire e contribuire alle attività di revisione ed ispezione effettuate dal titolare, prestando assistenza a quest'ultimo nell'evasione delle richieste formulate da parte degli interessati;
   f) ad informare il titolare in caso di violazione dati e ad assisterlo nella valutazione di impatto dei rischi.

Articolo 11 - Responsabile esterno del trattamento dei dati personali

1. É responsabile esterno del trattamento qualunque soggetto esterno che esegue, in base a un contratto, una convenzione o altro atto giuridico, trattamenti di dati personali per conto dell'Università e risponde in solido con l'Università in caso di inosservanza di obblighi normativi.
2. Il responsabile esterno del trattamento è nominato con atto giuridico conforme alla normativa vigente[3]; in particolare per quel che riguarda le misure tecniche e organizzative adeguate a consentire il rispetto delle disposizioni previste nel presente regolamento.
3. Il responsabile esterno può nominare, mediante contratto o altro atto giuridico, sub-responsabili del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che lo legano all'Università.
4. Qualora un sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile esterno originario rimane interamente responsabile nei confronti dell'Università dell'adempimento degli obblighi da parte dei sub-responsabili dal medesimo nominati.
5. Il responsabile esterno risponde nei confronti dell'Università dell'inadempimento del sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento.

Articolo 12 - Amministratore di sistema

[2] Articolo 28, comma 3, del regolamento UE
[3] Articolo 28, comma 3 del regolamento UE

1. L' amministratore di sistema è la persona autorizzata alla gestione e alla manutenzione di un impianto di elaborazione o di suoi componenti, con cui vengono effettuati trattamenti di dati personali.
2. E' designato dal titolare con un atto che individua analiticamente i compiti e gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Articolo 13 - Persone autorizzate al trattamento

1. Le persone autorizzate al trattamento sono i componenti della comunità universitaria che per la loro funzione o incarico hanno accesso a dati personali.
2. Il trattamento deve essere effettuato secondo le istruzioni del titolare, del designato, del responsabile del trattamento o di chiunque agisca sotto la loro autorità.
3. Le persone autorizzate al trattamento ricevono formazione e informazione specifica in materia di protezione dei dati.
4. Le persone autorizzate effettuano i trattamenti dei dati personali in osservanza delle misure di sicurezza previste dall'Università al fine di evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito dei dati personali.
5. Le persone autorizzate sono tenute:
   a) a mantenere il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni di cui siano venute a conoscenza durante l'attività prestata;
   b) a non comunicare a terzi o diffondere con o senza strumenti elettronici le notizie, informazioni o dati appresi in relazione a fatti e circostanze di cui siano venute a conoscenza;
   c) a seguire i seminari d'informazione e formazione in materia di protezione dei dati e a sostenere i relativi test finali per la verifica dell'apprendimento;
   d) a segnalare con tempestività al proprio responsabile di ufficio e al referente eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare, nei casi di rischio grave per i diritti e le libertà delle persone fisiche, le procedure di comunicazione delle violazioni di dati al Garante per la privacy e ai soggetti interessati (istituto del data breach).
6. Le persone autorizzate al trattamento sono informate e consapevoli che l'accesso e la permanenza nei sistemi informatici dell'Ateneo per ragioni estranee o diverse rispetto a quelle per le quali sono stati abilitati per fini istituzionali e di servizio può configurare il reato di accesso abusivo ai sistemi informatici, può comportare sanzioni disciplinari, oltre che l'obbligo di risarcimento del danno a seguito dell'esposizione dell'amministrazione a pregiudizi reputazionali o di immagine.
7. Le persone autorizzate si impegnano a osservare, le politiche, i regolamenti e le istruzioni in materia di sicurezza informatica adottate dall'Università.
8. Nel caso in cui non ricorrano le condizioni di cui al presente articolo, coloro che, nello svolgimento dei propri compiti, vengano a conoscenza di dati personali al cui trattamento non possiedono esplicita autorizzazione o il cui trattamento non compete alla unità organizzativa cui afferiscono, sono considerati alla stregua di soggetti terzi rispetto all'amministrazione stessa, con l'applicabilità dei conseguenti limiti per quanto concerne la comunicazione e l'utilizzazione dei dati e la liceità del trattamento.

Articolo 14 - Referente per il trattamento dei dati personali

1. Il designato al trattamento individua tra i membri del personale della propria struttura un referente avente la funzione di coordinare le azioni necessarie all'applicazione della normativa in materia di protezione dei dati tra cui la ricognizione dei trattamenti svolti, l'adeguamento della modulistica e degli adempimenti previsti dalla normativa. Il referente favorisce, inoltre, il flusso di informazioni verso il RPD.

Titolo IV

Regole sul trattamento di dati

Articolo 15 - Circolazione interna dei dati personali

1. La comunicazione dei dati personali tra le strutture dell'Università è consentita per il perseguimento delle finalità istituzionali e secondo il principio di libera circolazione delle informazioni all'interno dell'Ateneo. La richiesta di accesso ai dati può essere formulata senza formalità, ma deve essere motivata da finalità istituzionali. Se è avanzata per finalità ulteriori, la richiesta deve essere scritta e motivata.
2. Ai fini del presente regolamento, sono equiparati alle strutture dell'Università gli organismi di controllo e valutazione quali il Collegio dei revisori, il Nucleo di valutazione e il Presidio di qualità.

Articolo 16 - Tipologie di dati trattati dall'Università

1. Per il perseguimento dei propri fini istituzionali, l'Università tratta i dati personali secondo quanto disposto da norme di legge e di regolamento. A titolo esemplificativo e non esaustivo, il predetto trattamento comprende:

a) dati, anche di natura particolare, relativi al personale dipendente o con rapporto di lavoro autonomo, ivi compresi i soggetti il cui rapporto di lavoro sia cessato o altro personale operante a vario titolo nell'Università, quali:
   - prove concorsuali/selezioni;
   - gestione del rapporto di lavoro;
   - formazione e aggiornamento professionale;
   - gestione di progetti di ricerca;
   - monitoraggio e valutazione della ricerca;
   - attività di trasferimento tecnologico;
   - politiche welfare e per la fruizione di agevolazioni;
   - salute e la sicurezza delle persone nei luoghi di lavoro;
   - erogazione del servizio di telefonia fissa e mobile;

b) dati relativi agli studenti, intesi nell'accezione più ampia, per tutte le attività e modalità connesse alla qualifica di studente o di laureato, quali:
   - attività di orientamento;
   - erogazione dei test di ingresso o alla verifica dei requisiti di accesso;
   - -erogazione del percorso formativo e gestione della carriera (dall'immatricolazione alla laurea);
   - attività di tirocinio;
   - attività di job placement;
   - attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community;
   - rilevazioni statistiche e valutazione della didattica;
   - diffusione dell'elaborato finale o di elementi ad esso connessi;
   - servizi di tutorato, assistenza, inclusione sociale;
   - servizi e attività per il diritto allo studio;
   - procedimenti di natura disciplinare a carico di studenti;

c) dati relativi alla didattica e alla ricerca (compresa la ricerca in ambito medico-sanitario);

d) dati relativi alle attività gestionali, conto terzi e/o connesse ad attività trasversali, quali:
   - gestione degli spazi;
   - gestione delle postazioni;
   - gestione degli organi e delle cariche istituzionali;
   - gestione degli infortuni;
   - servizi bibliotecari;

- servizi di protocollo e conservazione documentale;
- acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso;
- servizi di posta elettronica e strumenti di collaboration;
- erogazione federata di servizi;
- erogazione del servizio Eduroam;
- accesso a servizi federati;
- tracciamento di informazioni non primarie.

Articolo 17 - Comunicazione e diffusione dei dati personali

1. Le richieste di soggetti esterni all'Università finalizzate a ottenere la comunicazione o la diffusione di dati personali devono essere scritte, motivate, e contenere:
   a) il nome, la denominazione o la ragione sociale del richiedente;
   b) la tipologia di dati, le finalità e le modalità di utilizzo dei dati;
   c) l'eventuale ambito e la forma, se anonima e/o aggregata, di comunicazione e diffusione dei dati richiesti;
   d) la dichiarazione che il richiedente si impegna a utilizzare i dati ricevuti esclusivamente per le finalità e con le modalità di trattamento indicate nella richiesta.
2. Il designato, dopo avere valutato che la richiesta dei dati è compatibile con i fini istituzionali dell'Università e conforme alla normativa vigente, provvede alla trasmissione dei dati nella misura e secondo le modalità strettamente necessarie a soddisfare la richiesta.
3. Le richieste provenienti da pubbliche amministrazioni sono soddisfatte quando risultano necessarie al perseguimento dei fini istituzionali dell'ente richiedente, in base a quanto dichiarato dall'ente stesso.
4. L'Università può comunicare e diffondere, previa informativa, anche all'estero, dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali, diversi da categorie particolari di dati individuati dalla normativa[4] e da dati relativi a condanne penali e reati[5], anche a privati e per via telematica, al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, tale finalità deve essere dichiarata nella richiesta.
5. La comunicazione e la diffusione dei dati da parte dell'Università sono comunque autorizzate quando siano previste dalla normativa europea ovvero da norme di legge o di regolamento.

Articolo 18 - Diritti degli interessati

1. L'Università garantisce il rispetto dei diritti degli interessati.
2. Pertanto, l'interessato può:
   a) ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e la loro descrizione nel dettaglio, ove possibile ai sensi della normativa vigente;
   b) ottenere l'accesso, la rettifica, la cancellazione dei propri dati nonché presentare opposizione al loro trattamento;
   c) esercitare il diritto alla limitazione del trattamento non solo in caso di violazione dei presupposti di liceità dello stesso e quale alternativa alla cancellazione dei dati stessi, ma anche nell'attesa della valutazione da parte del titolare della richiesta di rettifica dei dati o di opposizione al trattamento. In condizioni di limitazione e con la sola eccezione della conservazione, ogni altro trattamento del dato è consentito solo in presenza del consenso dell'interessato o dell'accertamento dei diritti in sede giudiziaria, di tutela dei diritti di altra persona fisica o giuridica o in presenza di un interesse pubblico rilevante;
   d) esercitare il diritto di opposizione alla profilazione;

[4] Articolo 9 del regolamento UE
[5] Articolo 10 del regolamento UE

e) esercitare il diritto alla portabilità dei dati solo qualora il trattamento si basi sul consenso o su un contratto e sia effettuato con mezzi automatizzati; tale diritto non si applica al trattamento necessario per l'esecuzione dei compiti di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita l'Università;
f) esercitare il diritto all'oblio chiedendo la cancellazione dei propri dati personali nel caso questi siano stati resi pubblici on-line. Tale diritto può essere esercitato ove ricorra una delle seguenti fattispecie:
   - i dati personali non sono più necessari rispetto alle finalità per cui sono stati raccolti;
   - l'interessato revoca il consenso su cui si basa il trattamento;
   - l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
   - i dati personali sono trattati illecitamente;
   - si tratti di adempiere ad un obbligo legale;
   - i dati riguardino minori.

2. L'Università informa della richiesta di cancellazione ogni altro eventuale titolare che tratta i dati personali cancellati, compresi qualsiasi collegamento, copia o riproduzione.
3. L'interessato può esercitare i suoi diritti con richiesta scritta indirizzata al responsabile della struttura competente per il trattamento dei dati personali oggetto della richiesta o in alternativa al designato o al suo referente.
4. Il riscontro alla richiesta presentata dall'interessato viene fornito dal designato entro trenta giorni dalla data di protocollazione della richiesta, anche nei casi di diniego. Nei casi di particolare e comprovata difficoltà, il termine di trenta giorni può essere prorogato fino a tre mesi. Di tale proroga viene data informazione all'interessato entro trenta giorni dalla richiesta.
5. Il riscontro fornito all'interessato deve essere espresso con linguaggio semplice e chiaro.
6. L'Università agevola, per il tramite dei designati, l'esercizio dei diritti da parte dell'interessato, adottando ogni necessaria misura tecnica e organizzativa.
7. L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato.
8. Nel caso in cui le richieste siano manifestamente infondate, eccessive o ripetitive, l'Università può porre a carico del richiedente un contributo spese proporzionato ai costi amministrativi sostenuti, oppure può rifiutare di soddisfare la richiesta, dimostrando il carattere manifestamente infondato o eccessivo della stessa. Con provvedimento del Direttore generale sono definiti gli importi dei contributi spese e delle relative modalità di pagamento.

Articolo 19 - Informativa

1. Per ogni tipologia di trattamento dei dati l'Università fornisce l'informativa all'interessato, salvo il caso in cui l'interessato sia già in possesso delle informazioni o in altri casi particolari previsti dalla normativa vigente.[6]
2. L'informativa fornita all'interessato deve essere concisa, trasparente, intellegibile, facilmente accessibile e redatta con un linguaggio chiaro e semplice.
3. L'informativa deve contenere:
   a) i dati di contatto dell'Università;
   b) i dati di contatto del RPD;
   c) le finalità del trattamento;
   d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e, nel caso in cui i dati personali non siano raccolti presso l'interessato, anche le categorie di dati trattati e le relative fonti di provenienza;

[6] Articolo 14, comma 5 del regolamento UE

e) l’eventuale volontà dell’Università di trasferire dati personali a un paese terzo o a un'organizzazione internazionale, il fondamento giuridico alla base di tale trasferimento, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili;
f) il periodo di conservazione dei dati personali oppure, in alternativa, i criteri utilizzati per determinare tale periodo;
g) i diritti che l’interessato può esercitare, quali: l’accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento o l’opposizione, il diritto alla portabilità dei dati, la revoca del consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca, il diritto di proporre reclamo al Garante per la protezione dei dati personali;
h) la necessità di comunicare i dati personali in base a un obbligo legale o contrattuale, nonché la natura obbligatoria o facoltativa del conferimento, nonché le possibili conseguenze dell’omessa comunicazione di tali dati;
i) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e le conseguenze previste da tale trattamento per l'interessato.

4. Nel caso in cui i dati personali debbano essere trattati per una finalità diversa da quella per cui sono stati raccolti, prima di procedere a tale ulteriore trattamento, l’Università fornisce all'interessato informazioni in merito alla diversa finalità.
5. Nel caso in cui i dati non siano raccolti presso l’interessato, l’Università si riserva la possibilità di non fornire l’informativa quando l’interessato disponga già delle informazioni o la comunicazione di tali informazioni risulti impossibile o risulti troppo impegnativa.
6. L’informativa può non essere fornita nel caso in cui si prefiguri il rischio di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità del trattamento.
7. Le informative di competenza delle strutture sono aggiornate dai designati interni.
8. La modulistica che prevede la raccolta di dati riferiti a una persona fisica deve contenere necessariamente le seguenti informazioni:
a) la finalità per cui i dati sono raccolti e per la quale saranno utilizzati;
b) l’indicazione di chi tratterà i dati all’interno dell’Università;
c) l’indicazione della possibilità che i dati siano resi disponibili a terzi;
d) l’espressione del consenso ove questo sia una condizione di liceità del trattamento.

Articolo 20 - Sensibilizzazione e formazione

1. Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, l’Università sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione finalizzato a consolidare la consapevolezza del valore della protezione dei dati personali. A tal fine, l’Università promuove una specifica attività formativa.
2. L’Università predispone periodicamente, sentito il RPD, un piano formativo in materia di trattamento dei dati personali e di prevenzione dei rischi di violazione, al fine di garantire una gestione responsabile, informata e aggiornata delle attività di trattamento. Tale formazione, sentito il Responsabile della anticorruzione e della trasparenza (RPCT), è integrata e coordinata con la formazione in materia di prevenzione della corruzione nonché con la formazione in tema di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza, accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera l’Università.
3. Ogni sessione formativa prevede, nell’ottica della responsabilizzazione, una prova finale di apprendimento.

4. La frequenza delle attività di formazione è obbligatoria e viene considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale.

Articolo 21 - Trattamenti nell'ambito del rapporto di lavoro

1. L'Università effettua il trattamento dei dati personali dei dipendenti, e di altri collaboratori, nell'ambito del rapporto di lavoro, adottando garanzie appropriate per assicurare la protezione dei diritti e delle libertà fondamentali della persona e nel rispetto della legge e dei contratti collettivi.
2. Il trattamento dei dati relativi ai dipendenti da parte dell'Università non richiede il consenso esplicito, in quanto il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza e protezione sociale.
3. L'Università garantisce ai dipendenti l'esercizio dei diritti previsti dalla normativa vigente[7], ivi compreso il diritto di accesso ai dati valutativi di natura soggettiva nonché il diritto all'informativa.
4. L'Università adotta misure tecniche e organizzative atte a garantire la tutela delle prerogative individuali e sindacali come disposte dalla normativa italiana, in particolare dallo Statuto dei lavoratori e dalle norme che lo richiamano, oltre che dalle regole deontologiche promosse dal Garante per la protezione dei dati personali.
5. L'Università può comunicare a soggetti pubblici e privati dati del personale che, in ragione di una qualifica professionale specifica, usufruisce di corsi di formazione forniti in accordo con altri enti pubblici, con lo scopo di migliorarne la fruibilità e di garantire la qualità e l'efficacia della formazione sul territorio nazionale.
6. L'Università comunica i dati del personale addetto alla sicurezza sui luoghi di lavoro a soggetti pubblici e privati che contribuiscono alla formazione specifica.
7. Nei casi di ricezione dei curriculum spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, l'informativa è fornita all'interessato al momento del primo contatto utile, successivo all'invio del curriculum stesso.
8. Non è dovuto il consenso al trattamento dei dati personali presenti nei curriculum quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.

Articolo 22 - Trattamento ai fini statistici o di ricerca scientifica

1. Il trattamento di dati personali ai fini statistici o di ricerca scientifica da parte di chiunque operi all'interno di uffici e strutture dell'Università o per conto dell'Università stessa, deve avvenire con le seguenti modalità:

a) i dati personali trattati a fini statistici o di ricerca scientifica non possono essere utilizzati per adottare decisioni o provvedimenti inerenti all'interessato, né trattati per altri scopi;
b) all'interessato deve essere fornita una puntuale informazione relativamente alle finalità statistiche o di ricerca scientifica del trattamento in conformità dell'articolo 19 del presente regolamento, a meno che la predetta informativa non richieda uno sforzo sproporzionato rispetto al diritto tutelato e sempre che siano adottate le idonee forme di pubblicità individuate dalle regole deontologiche in materia, promosse dal Garante.

2. Fuori dai casi di particolari indagini a fini statistici o di ricerca scientifica previste dalla legge, nei casi in cui sia richiesto, il consenso dell'interessato al trattamento di categorie particolari di dati personali può essere prestato con modalità semplificate, individuate dalle regole deontologiche previste dalla normativa vigente.

Articolo 23 - Trattamento ai fini di ricerca medica, biomedica, ed epidemiologica

[7] Dall'articolo 12 all'articolo 22 del regolamento UE

1. Non è necessario il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione Europea, ivi incluso il caso in cui la ricerca rientri in un programma di ricerca biomedica o sanitaria[8] e sia condotta e resa pubblica una valutazione d'impatto[9].
2. Il consenso non è, altresì, necessario quando, a causa di particolari ragioni, informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato oppure vi sia un rischio reale di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il responsabile scientifico della ricerca adotta misure idonee a tutelare i diritti, le libertà e i legittimi interessi dell'interessato. Il progetto di ricerca deve essere sottoposto alla preventiva consultazione del Garante per la protezione dei dati personali.
3. In caso di esercizio del diritto di rettifica e integrazione dei dati personali da parte dell'interessato, la rettifica e l'integrazione dei dati sono annotate senza modificare questi ultimi, quando il risultato di tali operazioni non produca effetti significativi sul risultato della ricerca.
4. Ai fini del trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici, si applica la disciplina prevista dalla normativa vigente[10].

Articolo 24 - Trattamento ai fini di archiviazione nel pubblico interesse o di ricerca storica
1. I documenti contenenti dati personali, trattati a fini di archiviazione nel pubblico interesse o di ricerca storica, possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento di tali scopi.
2. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato garantendo il rispetto del principio della minimizzazione dei dati.
3. Ove possibile, e senza pregiudicare il raggiungimento delle finalità del trattamento, i dati dovranno essere trattati con misure tecniche che non consentano più di identificare l'interessato.
4. I dati personali raccolti a fini di archiviazione nel pubblico interesse o di ricerca storica non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalità secondo i principi stabiliti dalla normativa vigente.
5. Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato nel rispetto delle regole deontologiche in materia approvate dal Garante per la protezione dei dati personali.
6. La consultazione dei documenti di interesse storico conservati negli archivi dell'Università è disciplinata dalla normativa vigente[11], dalle relative regole deontologiche e dai regolamenti di Ateneo in materia.

Articolo 25 - Comunicazione e diffusione dei dati relativi ad attività didattica e di ricerca
1. Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico, l'Università può comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione dei dati di cui all'articolo 6 del presente regolamento.
2. L'Università può comunicare dati inerenti alla produttività scientifica, ai riconoscimenti e ai fondi acquisiti da singoli, gruppi o specifici settori scientifico-disciplinari, anche nell'ambito di procedure di valutazione di richieste di finanziamento o di progetti di ricerca, al fine di:

a) promuovere modelli di programmazione delle attività di ricerca e di allocazione delle risorse secondo meccanismi che consentano di garantire la trasparenza nella definizione delle

[8] Articolo 12-bis del d.lgs. n. 502/1992 "Riordino della disciplina in materia sanitaria, a norma dell'articolo 1 della legge 23 ottobre 1992, n. 421"
[9] Articoli 35 e 36 del regolamento UE
[10] Articolo 110-bis del codice in materia di protezione dei dati personali
[11] D.lgs. n. 42/2004 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137"

priorità, di valorizzare adeguatamente le capacità dei singoli e dei gruppi e di rispettare i principi di trasparenza ed equità di trattamento;
b) favorire la cooperazione tra singoli e gruppi mediante una precisa conoscenza dei risultati conseguiti, allo scopo di migliorare la capacità di attrarre finanziamenti esterni o di istituire forme di collaborazione strutturata con soggetti terzi;
c) fornire orientamento e sostegno per lo sviluppo di modelli organizzativi di supporto alla ricerca, anche tramite la realizzazione di analisi comparative e la condivisione di buone pratiche.

3. I dati aventi oggetto la valutazione dell'attività scientifica e didattica effettuata per conto dell'Università di Pisa possono essere resi pubblici esclusivamente nelle forme che assicurano la riservatezza dei singoli.
4. L'Università può comunicare dati personali, preferibilmente in forma anonima e aggregata, a soggetti pubblici che abbiano erogato finanziamenti per la ricerca, per finalità di rendicontazione e di elaborazione statistica.

Articolo 26 - Trattamento dei dati nelle sedute degli organi collegiali di Ateneo
1. Il trattamento dei dati nel corso delle sedute degli organi collegiali avviene solo per finalità istruttorie e deliberative, nel rispetto di quanto disposto dal presente regolamento.

Articolo 27 - Diffusione delle valutazioni d'esame
1. In ottemperanza ai principi di trasparenza cui l'Università si ispira e al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, è consentita la pubblicazione dei dati inerenti alle valutazioni d'esame anche sui siti web di Ateneo, in una sezione accessibile utilizzando le credenziali di ateneo.
2. La pubblicazione dei dati sui siti web è consentita unicamente mediante l'indicazione del numero di matricola dello studente e del voto conseguito nelle prove intermedie e finali.
3. Le valutazioni sono rese disponibili per un periodo di tempo non superiore all'anno accademico di riferimento.

Articolo 28 - Diffusione dei risultati dei concorsi e selezioni
1. In ottemperanza ai principi di trasparenza, l'Università è tenuta a pubblicare gli esiti delle procedure di reclutamento del personale o le procedure di selezione per l'ammissione a corsi a numero programmato o per il conferimento di assegni di ricerca, borse di dottorato o di studio, incarichi di collaborazione e/o insegnamento, nonché le relative graduatorie, anche sui siti web di Ateneo.
2. La pubblicazione dei dati sui siti web è effettuata nel rispetto del principio della minimizzazione dei dati, mediante l'indicazione dei dati strettamente necessari al raggiungimento delle finalità per le quali sono pubblicati.
3. La pubblicazione dei dati di cui al presente articolo perdura per il periodo di tempo previsto dalla normativa vigente in materia di trasparenza.

Articolo 29 - Registro delle attività di trattamento
1. L'Università istituisce un registro delle attività di trattamento svolte sotto la propria responsabilità.
2. Il Registro è assunto agli atti dell'Università con data certa.
3. Il registro censisce le attività di trattamento svolte dagli uffici e dalle strutture dell'Università e le principali caratteristiche di tali attività.
4.Il registro è periodicamente aggiornato, secondo le istruzioni del RPD, e, su richiesta, è messo a disposizione del Garante per la protezione dei dati personali.
5. Nel registro sono elencati e descritti sia i trattamenti dei quali l'Università è titolare, sia i trattamenti che l'Università effettua in qualità di responsabile esterno di altri titolari.

5a) Il registro dei trattamenti dei quali l'Università è titolare contiene le seguenti informazioni:

- le strutture competenti al trattamento;
- le finalità del trattamento;
- la descrizione delle categorie di interessati nonché le categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, il richiamo alle misure di sicurezza tecniche ed organizzative adottate in sede di trattamento.

5b) Il registro dei trattamenti svolti dall'Università per conto di altri titolari e per i quali l'Università si configura come responsabile contiene le seguenti informazioni:

- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per quanto riguarda i trasferimenti di cui all'articolo 49, comma 2, del regolamento UE, la documentazione delle garanzie adeguate;
- il richiamo alle misure di sicurezza tecniche ed organizzative adottate in sede di trattamento.

Articolo 30 - La valutazione di impatto sulla protezione dati

1. Quando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità del trattamento e l'utilizzo di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il designato, previa consultazione con il RPD e prima di procedere al trattamento, è tenuto ad effettuare la valutazione dell'impatto sulla protezione dei dati personali.
2. È possibile condurre una singola valutazione di impatto per un insieme di trattamenti simili che presentano rischi di analogo livello elevato.
3. La valutazione d'impatto sulla protezione dei dati è obbligatoria in caso di:

a) valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) trattamento, su larga scala, di categorie particolari di dati personali quali: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati relativi a condanne penali e a reati;
c) sorveglianza sistematica su larga scala di una zona accessibile al pubblico (videosorveglianza);
d) trattamento di dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico o epidemiologico.

4. Il designato si consulta con il RPD anche per assumere la decisione di effettuare o meno la valutazione di impatto. Tale consultazione e le conseguenti decisioni assunte dal designato devono essere documentate nell'ambito della valutazione di impatto. Il designato è tenuto a motivare decisioni o condotte difformi da quelle raccomandate dal RPD.
5. Il responsabile per la sicurezza e per la transizione al digitale fornisce supporto ai designati o ai loro referenti e al RPD per lo svolgimento della valutazione del rischio.
6. Se le risultanze della valutazione di impatto (di seguito DPIA) indicano l'esistenza di un rischio residuale elevato, prima di procedere al trattamento l'Università, per il tramite del RPD, consulta il Garante per la protezione dei dati personali.

7. L'Università, per il tramite del RPD, consulta il Garante per la protezione dei dati personali anche nei casi in cui la vigente legislazione stabilisca l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, in merito a trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica. In particolare, la consultazione è obbligatoria ove non sia necessario il consenso per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico.

Articolo 31 – Videosorveglianza

1. Il trattamento dei dati personali effettuato mediante impianti di videosorveglianza negli ambienti dell'Università si svolge nel rispetto dei diritti, delle libertà fondamentali nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale, garantendo, altresì, i diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento.
2. Le immagini e i dati raccolti tramite gli impianti di videosorveglianza non possono essere utilizzati per finalità diverse da quelle indicate nella normativa vigente e nella disciplina di Ateneo in materia di videosorveglianza e non possono essere diffusi o comunicati a terzi, salvo in caso di indagini di polizia giudiziaria.
3. L'Università garantisce la protezione e la sicurezza dei dati personali raccolti attraverso sistemi di videosorveglianza. In particolare:

- tutto il personale coinvolto nelle operazioni di registrazione, visualizzazione e registrazione delle immagini, nonché il personale addetto alla manutenzione degli impianti e alla pulizia dei locali riceve una adeguata formazione sui comportamenti da adottare nel rispetto della normativa vigente in tema di protezione dei dati personali;
- solo il personale autorizzato può avere accesso alle immagini;
- il personale autorizzato è tenuto al segreto professionale;
- le immagini non possono essere conservate per un periodo più lungo del necessario, in conformità di quanto previsto dai principi applicabili al trattamento dei dati personali.

4. Nel caso in cui siano conservate per un periodo maggiore di quello previsto dall'apposito regolamento, le immagini devono essere custodite in un luogo sicuro con accesso controllato ed essere cancellate non appena la loro conservazione non sia più necessaria.
5. È onere del responsabile del trattamento per la videosorveglianza di Ateneo:

a) adottare le garanzie di cui all'articolo 4, legge 20 maggio 1970, n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
b) garantire l'osservanza dei principi di necessità, finalità e proporzionalità del trattamento dei dati;
c) garantire il rispetto del presente regolamento, delle prescrizioni imposte dal Garante e dalla normativa vigente, anche in relazione all'utilizzazione di particolari tecnologie e/o apparecchiature;
d) redigere un documento in cui siano esposte le ragioni dell'installazione di tali sistemi anche ai fini dell'eventuale esibizione in occasione di visite ispettive oppure dell'esercizio dei diritti dell'interessato o in caso di contenzioso.

5. Resta ferma la necessità di effettuare una valutazione del rischio ogni qualvolta vengano installate apparecchiature di videosorveglianza in ambienti o zone accessibili al pubblico.
6. Non è consentito, nel rispetto dello Statuto dei lavoratori, l'uso di impianti e apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.

Titolo V
Misure di sicurezza

Articolo 32 – Sicurezza

1. L'Università mette in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio di lesione dei diritti e delle libertà delle persone fisiche.
2. Nel valutare l'adeguato livello di sicurezza, l'Università tiene conto dei rischi che derivano in particolare dalla distruzione, perdita, modifica, divulgazione non autorizzata o accesso, accidentale o illecito, a dati personali trasmessi, conservati o comunque trattati.
3. L'Università, per il tramite del Gruppo Sicurezza ICT coordinato dal responsabile della sicurezza informatica, effettua la valutazione dei rischi connessi al trattamento e adotta misure di sicurezza comprendenti, tra le altre:

- la pseudonimizzazione e la cifratura dei dati,
- le misure implementative della riservatezza, dell'integrità, della disponibilità delle informazioni;
- la resilienza dei sistemi e delle applicazioni di trattamento nonché il loro tempestivo ripristino in caso di incidente fisico o tecnico;
- l'adozione di procedure idonee a testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

4. L'Università considera rischioso il trasporto di dati personali su ogni supporto (computer portatili, copie cartacee, pendrive ecc.). Ciò vale prioritariamente per le categorie particolari di dati, i grandi volumi di dati personali e le informazioni che comportano particolari rischi per l'interessato nel caso di perdita o distruzione. Solo in circostanze eccezionali tali dati possono essere trasportati fuori dagli ambienti dell'Università e sotto la diretta responsabilità di personale autorizzato. In particolare, il personale autorizzato è tenuto a:

- ove possibile, fare uso di accesso remoto tramite login e password alle informazioni;
- trasportare solo la quantità minima di dati personali;
- assicurarsi che i dispositivi mobili e i dispositivi di archiviazione esterna utilizzati per il trasporto di dati personali all'esterno di ambienti universitari siano dotati di sistemi di crittografia e il loro accesso sia protetto da password, PIN o qualsiasi altro meccanismo che impedisca l'accesso non autorizzato.

5. Qualunque perdita e/o furto di dati deve essere tempestivamente segnalato e trattato secondo la procedura di gestione delle violazioni di dati personali di cui all'articolo 33 del presente regolamento.
6. Per quanto non espressamente disciplinato dal presente articolo in tema di sicurezza, si rinvia a quanto disposto dai regolamenti di Ateneo in materia e, in particolare, da quelli emanati in osservanza delle previsioni del Documento programmatico per la sicurezza e dalle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" predisposte da AgID (Agenzia per l'Italia Digitale).
7. Il trattamento dei dati personali contenuti nei log dei sistemi informatici è consentito in misura strettamente necessaria e proporzionata al fine di garantire la sicurezza dei sistemi stessi.

Articolo 33 - Violazione di dati personali (Data Breach)

1. Per violazione dei dati personali si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
2. Al fine di tutelare le persone, i dati e le informazioni e di documentare i flussi per la gestione delle violazioni dei dati personali trattati, l'Università, in qualità di titolare del trattamento, definisce una procedura di gestione delle violazioni di dati personali.
3. Tale procedura si applica a qualunque attività svolta dall'Università e, in particolare, a tutti gli archivi e/o documenti cartacei e a tutti i sistemi informativi attraverso cui sono trattati dati personali, anche con il supporto di fornitori esterni.
4. La procedura definisce le modalità con cui identificare la violazione, analizzare le cause di quest'ultima, definire le misure da adottare per rimediare alla violazione dei dati personali, attenuarne

i possibili effetti negativi, registrare le informazioni relative alla violazione, identificare le azioni correttive e valutarne l'efficacia, notificare la violazione di dati personali al Garante nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche, comunicare una violazione dei dati personali all'interessato nel caso in cui il rischio sia elevato.
5. La procedura è stabilita dal Responsabile alla Transizione Digitale in collaborazione col Responsabile per la Sicurezza ed è resa disponibile attraverso la rete intranet di Ateneo.
6. La procedura costituisce una delle materie oggetto della formazione del personale di cui all'art 13 del presente regolamento.
7. Il rispetto della procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento ivi previste può comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo la normativa vigente in materia.

Titolo VI
Disposizioni comuni e finali

Articolo 34 - Violazioni e forme di responsabilità
1. Ferma l'applicabilità della disciplina prevista dalla vigente normativa europea e nazionale in materia[12], la violazione delle leggi, del presente regolamento e delle procedure in tema di protezione dei dati personali da parte dei dipendenti, costituisce violazione dei doveri di ufficio e comporta responsabilità disciplinare; può dar luogo, altresì, a responsabilità penale, civile e amministrativa.
2. La violazione da parte dei dipendenti delle leggi, del presente regolamento e delle procedure in tema di protezione dei dati personali costituisce, altresì, violazione del codice etico di Ateneo.

Articolo 35 - Divieto di indennità
1. Nel rispetto della normativa vigente, ogni incarico previsto dal presente regolamento non dà diritto ad indennità alcuna, né a gettoni di presenza.

Articolo 36 - Disposizioni finali
1. Il presente regolamento, acquisito il parere del Consiglio di amministrazione, è approvato dal Senato accademico ed emanato con decreto rettorale.
2. Dalla data di entrata in vigore del presente regolamento, devono intendersi abrogate tutte le norme regolamentari incompatibili in relazione a soggetti e materie interessati al trattamento.
3. Per quanto non espressamente previsto dal presente regolamento, si rinvia alle disposizioni del regolamento UE n. 679/2016 e del decreto legislativo 30 giugno 2003, n.196, oltre che a quanto previsto dalle linee guida e di indirizzo e dalle regole deontologiche adottate e approvate dal Garante.
4. Costituiscono parte integrante e sostanziale del presente regolamento tutti gli allegati che ad esso si riferiscono in quanto connessi ad ambiti specifici in esso contenuti, anche redatti successivamente alla sua emanazione.

Articolo 37 - Efficacia temporale e pubblicità
1. Il presente regolamento entra in vigore 15 giorni dopo la sua pubblicazione all'Albo Ufficiale Informatico. Il presente regolamento è consultabile sul sito web di Ateneo.

[12] Articoli 58, 82, 83 e 84 del regolamento UE e codice in materia di protezione dei dati personali