Data Protection Master Policy

Data di emissione e decorrenza	03/06/2020
Numero revisione	
Revisione	
Preparata da	
Controllata da	
Approvata da	

Sommario

1. INTRODUZIONE 3
1.1 NORMATIVA APPLICABILE 3
1.2 SCOPO 3
1.3 DESTINATARI E CONSEGUENZE IN CASO DI MANCATO RISPETTO DELLA *POLICY* 4
2. DEFINIZIONI 4
3. LE REGOLE GENERALI DEL TRATTAMENTO 7
3.1 IL PRINCIPIO DI *ACCOUNTABILITY* 7
3.2 I PRINCIPI GENERALI DA RISPETTARE NEL TRATTAMENTO DEI DATI 7
3. 3 PRINCIPI DA ATTUARE NELL'ORGANIZZAZIONE DEL TITOLARE 8
4. LA *PRIVACY GOVERNANCE* DI ESU 9
4.1 IL TITOLARE ED IL DELEGATO *PRIVACY* 9
4.2 IL RUOLO DEI SOGGETTI "REFERENTI PRIVACY" 9
4.3 I SOGGETTI AUTORIZZATI AL TRATTAMENTO 10
4.5 IL DATA PROTECTION OFFICER (DPO). 10
4.6 IL RUOLO E LA SCELTA DEI RESPONSABILI 11
5. GLI INTERESSATI 11
5.1 TRATTAMENTO NEI CONFRONTI DI STUDENTI E OSPITI (*OSPITI, UTENTI, E IN GENERALE TUTTI I SOGGETTI CHE USUFRUISCONO DEI SERVIZI OFFERTI DALL'ENTE*) 12
5.1.1 L'informativa *13*
5.1.2 I cookie *13*
5.1.4 I diritti degli Studenti e Ospiti *14*
5.2 TRATTAMENTO NEI CONFRONTI DI DIPENDENTI, COLLABORATORI E CANDIDATI 14
5.2.1 L'Informativa Candidati *15*
5.2.2 L'Informativa Dipendenti e Collaboratori *16*
5.2.3 Il consenso *16*
5.2.4 Il Regolamento per l'utilizzo degli strumenti aziendali *16*
5.2.5 I diritti dei Dipendenti e Collaboratori *16*
5.3 I TERZI 16
5.3.1. L'Informativa *18*
5.3.2 I diritti dei Terzi *18*
6. GLI STRUMENTI DI TRATTAMENTO 18
6.1 IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DEL TITOLARE 18
6.2 *DATA BREACH* 18
6.3 *DATA PROTECTION IMPACT ASSESSMENT* (DPIA) 19
7. ALTRI TRATTAMENTI RILEVANTI 20
7.1 VIDEOSORVEGLIANZA 20
8. LA GOVERNANCE IT 20
8.1 I PRINCIPI DEL GDPR 20

1. Introduzione

1.1 Normativa applicabile

La Data Protection Master *Policy* (di seguito **"*Policy*"**) di ESU A.R.D.S.U. (di seguito, anche l'**"Ente"** o semplicemente "**ESU**") è adottata in attuazione del "*Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al Trattamento, nonché alla libera circolazione di tali Dati e che abroga la direttiva 95/46/CE ("General Data Protection Regulation*")" (di seguito **"GDPR"**).

Il GDPR prevede una disciplina uniforme in tema di *privacy*, valida in tutta l'Unione Europea, e ha lo scopo di assicurare all'interno della stessa un livello coerente ed elevato di protezione e la rimozione degli ostacoli alla circolazione dei Dati Personali.

Il GDPR è entrato in vigore il 24 maggio 2016 senza necessità di recepimento per mezzo di atti nazionali ed è applicabile in tutti i Paesi UE a partire dal 25 maggio 2018. L'Autorità Garante per la Protezione dei Dati Personali (di seguito il "**Garante**") ha adottato il 28 aprile 2017 una prima "*Guida all'applicazione del Regolamento europeo in materia di protezione dei Dati personali*", successivamente aggiornata (di seguito "**Guida all'applicazione del GDPR**").

Il 19 settembre 2018 è entrato in vigore il D.Lgs 101/2018 che contiene disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR che ha apportato significative modifiche al D.Lgs 196/2003 "*Codice in materia di protezione dei Dati personali*" (di seguito **"Codice Privacy"**), in vigore dal 1^ gennaio 2004.

La *Policy* è quindi redatta tenuto conto delle disposizioni del GDPR, del Codice Privacy, cosi come modificato dal D.Lgs 101/2018, nonché delle Linee Guida e dei Provvedimenti del Garante che resteranno in vigore (di seguito la **"Normativa Vigente"**).

1.2 Scopo

Lo scopo della *Policy* è quello di fornire il quadro relativo all'attuazione del GDPR all'interno dell'Ente. A tal riguardo, ai fini della predisposizione della *Policy* stessa, ESU ha condotto, nel corso del periodo luglio-settembre 2018, una attività di *Risk Assessment* che si è conclusa con la formalizzazione di un *report* che ha dato evidenza dello stato di adeguamento al Codice *Privacy*, del livello di maturità rispetto al GDPR (considerato parzialmente *compliant* alla data del 28 settembre 2018), dei relativi *gap* riscontrati e del conseguente *action plan* (di seguito il **"*Risk Assessment*"**).

Alla luce degli esiti di tale attività, l'Ente ha pertanto ritenuto, nell'ottica dell'*accountability*, di dotarsi dell'organizzazione *privacy* di seguito descritta.

Inoltre, l'Ente, che svolge attività volta a garantire e promuovere il Diritto allo Studio Universitario, nell'ambito delle competenze affidate all'ESU dalla Regione Veneto (Legge Regionale n. 8 del 7 aprile 1998), fornendo assistenza e sostegno agli studenti universitari mediante l'erogazione di benefici e servizi, tra cui l'ammissione alle residenze e alloggi universitari, l'erogazione di Borse di Studio e prestiti, nonché specifici interventi per studenti con disabilità, sulla base delle risultanze dell'attività di *Risk Assessment* condotte nel suddetto periodo, ha adottato un *set* di documenti conformi al GDPR (informative, nomine a responsabili,

policies varie, *etc*.) messi a disposizione dei Destinatari, come di seguito definiti, con le modalità specificate nel prosieguo.

In tal senso la *Policy* fornisce, altresì, indicazioni da parte dell'Ente in merito a come viene disciplinato il Trattamento (come di seguito definito) di Dipendenti e Collaboratori, Studenti e Ospiti, Fornitori nonché di altri soggetti eventualmente Interessati. Il trattamento è "disegnato" sulla base delle specifiche attività dell' Ente, come identificate nelle tabelle del paragrafo 5. L'Ente provvede al trattamento nell'ambito del perseguimento dei propri scopi, come risultanti dalle finalità istituzionali, nei limiti e secondo le regole previste nella *Policy* e nei relativi allegati, in conformità a quanto previsto dal GDPR.

1.3 Destinatari e conseguenze in caso di mancato rispetto della *Policy*

Le regole ed istruzioni contenute nella *Policy* sono rivolte a tutti i Dipendenti e collaboratori a qualsiasi titolo dell'Ente.

A tal fine si considerano:

- ✓ Dipendente/i: un dipendente, un candidato o un precedente dipendente dell'Ente, inclusi i lavoratori somministrati. La presente definizione non include i consulenti che prestano la propria attività presso l'Ente.
- ✓ Collaboratore/i: soggetti che collaborano con l'Ente, a prescindere dal rapporto contrattuale, come ad esempio gli studenti che prestano attività per conto dell'Ente (es. studenti 200 ore, stagisti, tirocinanti) e i consulenti.

La violazione della presente Policy può determinare l'applicazione da parte dell'Ente:

- ✓ di provvedimenti disciplinari a carico dei Dipendenti ;
- ✓ la risoluzione del contratto e le azioni conseguenti stabilite dalla legge, nei confronti dei Collaboratori.

2. Definizioni

Ai fini della *Policy* vengono definiti i seguenti termini:

Dati

- **Dati Personali:** qualsiasi informazione riguardante una persona fisica identificata o identificabile. L'identificazione della persona fisica può avvenire, direttamente o indirettamente, tramite Dati quali: nome per esteso, codice fiscale, numero di identificazione, numero di matricola; Dati di ubicazione; dati dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- **Categorie Particolari di dati:** dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- **Dati relativi alla salute**: dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

- **Dati genetici**: dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
- **Dati biometrici**: 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 personali relativi a condanne penali e reati:** informazioni relative a reati attribuiti o a condanne penali subite da una persona fisica, nonché qualsiasi altra informazione ritenuta sensibile ai sensi di legge.
- **Dati:** Dati Personali, Categorie Particolari di dati e dati relativi a condanne penali e reati considerati congiuntamente.

Soggetti

- **Titolare:** la persona (fisica o giuridica), l'autorità pubblica, o qualsiasi altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento.
- **Responsabile:** la persona (fisica o giuridica), l'autorità pubblica, il servizio o qualsiasi altro organismo, esterno all'Ente, che tratta Dati Personali per conto del Titolare del Trattamento, ai sensi dell'art. 28 del GDPR.
- **Sub-responsabile:** la persona (fisica o giuridica) nominata da parte di un Responsabile per specifiche attività di Trattamento, nel rispetto degli stessi obblighi contrattuali che legano Titolare e Responsabile.
- **Interessato/Interessati**: la persona fisica cui si riferiscono i Dati Personali.
- **DPO:** il Data Protection Officer[1], soggetto nominato dall'Ente in qualità di Responsabile della protezione dei Dati, qualora sussistano i requisiti previsti dall'articolo 37 del GDPR.
- **Amministratori di Sistema:** figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei Dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, secondo la definizione del Provvedimento del Garante del 27 novembre 2008 "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" (di seguito "**Provvedimento ADS**").
- **Garante Europeo**: l'autorità di sorveglianza indipendente che ha il compito di garantire che le istituzioni e gli organi dell'Unione Europea rispettino il diritto alla protezione dei dati in sede di Trattamento e di elaborazione di nuove politiche.

[1] (individuato nella traduzione italiana del Garante anche come "Responsabile Protezione dei Dati").

- **Autorità di Controllo** indica l'autorità pubblica indipendente istituita da uno Stato membro dell'Unione Europea.
- **Garante:** Garante per la protezione dei dati personali. Indica l'Autorità di Controllo italiana**.**
- **Personale** si riferisce, indistintamente, a Dipendenti e Collaboratori a qualsiasi titolo.

Modalità e strumenti a presidio del Trattamento

- **Trattamento:** trattamento dei Dati, ossia qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati o insiemi di Dati. Il Trattamento può svolgersi mediante 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 del Trattamento**: l'operazione con cui si contrassegnano alcuni Dati Personali trattati, con l'obiettivo di limitarne il Trattamento in futuro.
- **Profilazione:** qualsiasi forma di Trattamento automatizzato, con cui i Dati vengano utilizzati per valutare determinati aspetti di una persona fisica, in particolare per analizzare o prevedere il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti.
- **Pseudonimizzazione:** modalità di Trattamento effettuata in modo tale che i Dati non possano più essere attribuiti a un soggetto specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali Dati Personali non siano attribuiti a una persona fisica identificata o identificabile.
- **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, che i Dati Personali che lo riguardano siano oggetto di Trattamento.
- **Violazione dei Dati Personali ("*Data Breach*"):** una violazione in termini di sicurezza che comporti accidentalmente o in modo illecito: la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato a Dati Personali trasmessi, conservati o comunque trattati.
- **DPIA (acronimo di *Data Protection Impact Assessment*):** valutazione d'impatto sulla protezione dei dati.

3. Le regole generali del Trattamento

3.1 Il principio di *accountability*

Il GDPR impone un cambio di prospettiva ed un ruolo maggiormente attivo da parte dei Titolari nel Trattamento. In questo senso viene introdotto il concetto di "*accountability*" che si riferisce alla responsabilizzazione del Titolare stesso che deve farsi carico in prima persona di garantire il rispetto delle disposizioni a tutela dei Dati. Il Garante, nella Guida all'applicazione del GDPR, precisa che il Titolare deve attuare dei "*comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento*". La novità di questo principio consiste nell'attribuzione al Titolare del compito di decidere autonomamente le modalità, le garanzie e i limiti del Trattamento nel rispetto della Normativa Vigente.

Queste valutazioni devono essere svolte prima di procedere al Trattamento vero e proprio: è necessaria quindi un'analisi preventiva da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

A tal proposito l'Ente, come anticipato sopra, si è attivata mediante esecuzione di un *Risk Assessment* per conformare le procedure aziendali al GDPR.

Tutti i Destinatari devono essere pienamente consapevoli delle implicazioni connesse al Trattamento e delle regole di cui l'Ente stesso si è dotato al fine di garantire una adeguata tutela dei Dati stessi.

Nella gestione e manutenzione del modello *privacy* di cui l'Ente si è dotata, quest'ultima ha individuato nel Gruppo di Lavoro GDPR, composto da soggetti appartenenti al Settore Affari Generali, al Settore Diritto allo Studio, Settore Sistemi Informativi, eventualmente con il supporto del DPO, il compito di rivedere periodicamente – e comunque almeno una volta all'anno – lo stato di attuazione della Normativa Vigente. A tal fine il Gruppo di Lavoro utilizzerà il documento di *Risk Assessment* che si trova presso la funzione medesima approvato con Decreto del Direttore n. 6 del 8 gennaio 2019.

Al Gruppo di Lavoro GDPR è attribuito il compito di redigere/rivedere la documentazione in materia di data protection (informative, clausole contrattuali, Data Processing Agreement etc.…) – anche tramite consulenti incaricati dall'Ente – nonché di tenere l'archiviazione della suddetta documentazione e dei relativi aggiornamenti, anche in un database dedicato.

3.2 I principi generali da rispettare nel trattamento dei Dati

In estrema sintesi, i principi generali posti alla base di qualsiasi Trattamento, secondo il GDPR, sono:

a) liceità, correttezza e trasparenza: i Dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato. Il principio di liceità e correttezza prevede che i Dati di un Interessato possano essere trattati solo se questi: (i) ha espresso il proprio consenso al Trattamento per una o più specifiche finalità, (ii) quando il Trattamento è necessario all'esecuzione di un contratto di cui l'Interessato è parte, (iii) quando il Trattamento è necessario per adempiere un obbligo legale a cui è soggetto il Titolare; (iv) quando il Trattamento è necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica (v) quando è necessario per l'esecuzione di un compito di interesse pubblico o per il perseguimento del legittimo interesse del Titolare. Inoltre, in omaggio al principio di trasparenza, le modalità con cui sono raccolti e utilizzati i Dati devono essere trasparenti e le informazioni e comunicazioni relative al Trattamento devono esser altresì facilmente accessibili e comprensibili;

b) limitazione della finalità: i Dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in un modo che il relativo Trattamento non sia incompatibile con tali finalità. È considerato compatibile con le finalità inziali un ulteriore Trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;

c) minimizzazione dei Dati: i Dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati: il Trattamento deve avere ad oggetto solo la quantità di Dati necessaria per eseguire correttamente una determinata attività. Inoltre, i Dati raccolti per uno scopo non possono essere trattati per un altro scopo senza prima acquisire lo specifico consenso da parte dell'Interessato. L'Ente deve quindi limitare la raccolta, l'archiviazione e l'utilizzo dei Dati a quelli rilevanti, adeguati e assolutamente necessari per l'esecuzione dello scopo per il quale i dati vengono trattati;

d) esattezza: i Dati devono essere esatti e, se necessario, aggiornati; 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: i Dati devono essere conservati in una forma che consenta l'identificazione degli Interessati per un arco di tempo non superiore al tempo strettamente necessario al conseguimento delle finalità per le quali sono trattati. I Dati 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, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR a tutela dei diritti e delle libertà dell'Interessato;

f) integrità e riservatezza: i Dati devono essere trattati in maniera da garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate per proteggerli da Trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o dal danno accidentale.

3. 3 Principi da attuare nell'organizzazione del Titolare

In base all'art. 25, è necessario rispettare i principi che seguono:

a) *Privacy by design* (o 'fin dalla progettazione'): tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal Trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il Titolare mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione (la minimizzazione dei dati personali è uno dei principi generali in materia di privacy, fatto proprio dal nuovo GDPR. L'idea alla base della minimizzazione si ravvisa nella necessità di limitare le operazioni di trattamento a quanto effettivamente necessario per il perseguimento delle finalità del Titolare) e, a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli Interessati (art. 25, par. 1 GDPR).

b) *Privacy by default* (o 'per impostazione predefinita'): il Titolare mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del Trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure

garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza un intervento individuale (art. 25, par. 2 GDPR).

In caso di Trattamento effettuato mediante sito *web*, il soddisfacimento di questi adempimenti richiede un'ampia varietà di interventi, tra i quali ad esempio la configurazione dei sistemi in modo tale che i dati personali siano eliminati automaticamente alla scadenza del tempo di conservazione specificamente previsto per gli stessi.

4. La *Privacy Governance* di ESU

Dopo aver svolto l'attività di *Risk Assessment*, l'Ente ha ritenuto di dotarsi dell' organigramma *privacy*, come definito con DD n. 150 del 10.06.2019, con ciò intendendosi la struttura organizzativa a presidio dei processi legati alla *privacy.*

4.1 Il Titolare ed il Delegato *Privacy*

Ai fini dell'applicazione del GDPR, ESU è Titolare dei Dati trattati nello svolgimento delle proprie attività e contenuti nelle relative banche dati, sia su supporto elettronico che cartaceo.

Il Titolare opera per il tramite del proprio Direttore che è dotato dei poteri necessari all'adempimento degli obblighi previsti dalla Normativa Applicabile, come da Delibera del CdA del 13.05.2019 n. 38, compreso il potere di designare e preporre al trattamento dei Dati uno o più soggetti autorizzati, nonché i Responsabili esterni

4.2 Il ruolo dei soggetti "Referenti Privacy"

Costituisce una misura organizzativa idonea al rispetto della normativa del GDPR affidare compiti specifici sul Trattamento a figure interne qualificate dell'Ente, in ottemperanza al principio di *accountability* cui lo stesso GDPR è permeato.

L'Ente, nel dare attuazione alla regola di cui all'art. 29 del GDPR e all'art. 2-*quaterdecies* del Codice Privacy, ha ritenuto di modulare le istruzioni da fornire ai soggetti che devono trattare dati sotto la sua responsabilità, in modo da prevedere delle figure intermedie, dotate anche di compiti organizzativi.

Secondo l'Organigramma dell'Ente, il compito ed il potere di individuare Referenti Privacy è affidato al Direttore.

Il Direttore, nell'individuare i Referenti Privacy, deve prendere in considerazione soggetti in grado di fornire idonee garanzie in termini di esperienza, capacità ed affidabilità circa l'osservanza della normativa vigente e garantire il rispetto delle istruzioni ricevute, ivi compreso il profilo della sicurezza.

Per formalizzare l'incarico di Referenti Privacy, il Direttore utilizza il *template* di nomina allegato alla presente.

Il documento dovrà essere adattato a seconda dei compiti, coerenti con la propria funzione, che si vogliono affidare al nominando Referente Privacy. Per questa attività il Titolare coinvolge il Gruppo di Lavoro GDPR che fornirà supporto sia per la redazione della singola nomina che per il conseguente adattamento del documento.

Si allega il link, dal quale sono visualizzabili : 1) **il template di nomina dei Referenti Privacy;** 2) **elenco dei referenti**

http://cdv.esu.pd.it/L190/atto/show/96286?

4.3 I soggetti Autorizzati al Trattamento

Il GDPR, all'art. 29, precisa che chiunque agisca sotto l'autorità del Titolare e che abbia accesso ai Dati non può procedere al relativo Trattamento se non è debitamente istruito in tal senso dal Titolare medesimo.

Il Referente Privacy HR, coordinandosi con il Referente IT e con i responsabili di Settore, per quanto di competenza, ha il compito di identificare i dipendenti e i collaboratori a qualsiasi titolo dell'Ente idonei ad essere autorizzati al trattamento dei dati e di darne comunicazione al Titolare. L'ambito del Trattamento dell'Autorizzato viene individuato sulla base delle mansioni e degli applicativi a cui deve avere accesso lo stesso.

Il Titolare, con il supporto del Gruppo di Lavoro GDPR, procede alla nomina degli autorizzati.

Il Referente Privacy HR provvede ad aggiornare l'elenco degli Autorizzati, in occasione di qualunque modifica soggettiva del rapporto di lavoro od organizzativa, dandone tempestiva comunicazione al Titolare per gli adempimenti conseguenti. Il Referente Privacy HR provvede a darne comunicazione anche al Referente IT che procederà ad assegnare e/o disabilitare le credenziali di autenticazione.

S i allega il link, dal quale è visualizzabile **il template di nomina Autorizzato al trattamento**

http://cdv.esu.pd.it/L190/atto/show/96286?

4.4 Gli Amministratori di Sistema

La figura di Amministratore di Sistema è contenuta nel Provvedimento ADS e l'Ente ha ritenuto di mantenerla: ha infatti valutato che tale nomina contribuisse ad una corretta organizzazione dei ruoli *privacy* interna e costituisse, altresì, una adeguata misura di tutela dei Dati che la stessa tratta nello svolgimento della propria attività.

Le funzioni di **Amministratore di sistema** sono attribuite di norma al **Referente Privacy IT** il quale può nominare, per attività specifiche, altri amministratori di Sistema.

Gli Amministratori di Sistema devono adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (access log) devono presentare caratteristiche di completezza, inalterabilità e integrità tali da garantirne il raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non comunque superiore a sei mesi.

4.5 Il Data Protection Officer (DPO).

Il GDPR individua una nuova figura nell'ambito del governo della *privacy* (artt. 37-39 del GDPR) che dovrà:

- informare e fornire consulenza al Titolare in merito agli obblighi derivanti dalla Normativa Vigente;

- sorvegliare l'osservanza del GDPR da parte del Titolare, compresa l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa al Trattamento;
- fornire su richiesta pareri in merito alla valutazione d'impatto e sorvegliarne lo svolgimento;
- cooperare con il Garante fungendo, tra l'altro, da punto di contatto per questioni connesse al Trattamento, effettuando consultazioni di ogni tipo, con particolare riguardo e attenzione ad un'eventuale attività di consultazione preventiva.

La funzione del DPO può essere ricoperta da un soggetto con conoscenze specialistiche della normativa e delle prassi in materia di protezione dei Dati. Il DPO deve essere scelto in base alle sue qualità professionali ed alla sua preparazione in relazione alle operazioni di Trattamento, sia sul piano teorico che su quello pratico. Il DPO può essere un libero professionista, esterno e autonomo, incaricato in base a un contratto di servizi. Il GDPR prevede che il DPO debba essere obbligatoriamente nominato dal Titolare in tre occasioni:

1. Quando il Trattamento è effettuato da un'autorità pubblica o da un organismo pubblico (ad eccezione delle autorità giurisdizionali nell'esercizio delle loro funzioni);
2. Quando le attività principali del Titolare o del Responsabile consistono in Trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli Interessati su larga scala;
3. Quando le attività principali del Titolare o del Responsabile consistono nel Trattamento su larga scala, di Categorie particolari di dati personali (art. 9) o di Dati relativi a condanne penali e reati di cui all'articolo 10 GDPR.

In tutti gli altri casi la nomina del DPO è comunque facoltativa da parte del Titolare.

L'Ente, rientrando nel punto 1) ha provveduto a formalizzare la nomina, notificandola altresì al Garante Privacy.

4.6 Il ruolo e la scelta dei Responsabili

Qualora il Trattamento debba essere effettuato per conto dell'Ente da un soggetto ad essa terzo si procede a formalizzare con un contratto la nomina di quest'ultimo ai sensi dell'art. 28 del GDPR.

Questi soggetti devono offrire garanzie di esperienza, capacità ed affidabilità circa l'osservanza della Normativa Vigente nonché circa l'affidabilità sull'ottemperanza alle istruzioni ricevute.

Per formalizzare la nomina dovrà essere utilizzato il *template* allegato alla presente, (**Data_Processing_Agreement**).

5. Gli Interessati

Il GDPR, all'art. 6, prevede che il Trattamento è lecito ove sussista una delle seguenti condizioni:

a) L'Interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) 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;

c) Il Trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare;

d) Il Trattamento è necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;

e) Il Trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare;

f) Il Trattamento è necessario per il perseguimento del legittimo interesse del Titolare o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato che richiedono la protezione dei dati personali, in particolare se l'Interessato è un minore.

In riferimento alla propria attività istituzionale, l'Ente ha individuato, quali basi giuridiche del Trattamento, quattro categorie illustrate alle tabelle del successivo paragrafo (interesse pubblico, contratto, obbligo legale, legittimo interesse, così come richiamate rispettivamente alle lettere di cui sopra b), c), e, f)).

Le categorie di Interessati sono:

- **Studenti e Ospiti** (*ospiti, utenti, e in generale tutti i soggetti che usufruiscono dei servizi offerti dall'Ente*);
- **Dipendenti, Collaboratori, Candidati**;
- **Terzi:** Fornitori, stakeholders, membri del CdA;

In relazione agli utenti del sito *web* dell'Ente, si veda quanto descritto al paragrafo dedicato ai *cookie*.

5.1 Trattamento nei confronti di Studenti e Ospiti (*ospiti, utenti, e in generale tutti i soggetti che usufruiscono dei servizi offerti dall'Ente*)

		STUDENTI E OSPITI								
Dati Trattati		**Finalità**					**Base giuridica**			
		Garantire il diritto allo studio	**Fornire i servizi**	**Esecuzione del contratto**	**Tutela del Patrimonio**	**Obblighi Normativi**	**Interesse Pubblico**	**Contratto**	**Obbligo Legale**	**Legittimo interesse**
Anagrafici	SI	✓	✓			✓	✓		✓	
Di Contatto	SI	✓	✓			✓	✓		✓	
Relativi alla salute	SI	✓	✓			✓	✓		✓	
Condizione Economica	SI	✓	✓				✓			
Di Geolocalizzazione	NO									
Biometrici	NO									
Genetici	NO									
Relativi a condanne penali e reati	NO									
Bancari	NO	✓	✓							

Status di Studente e percorso accademico	SI	✓	✓			✓	✓			
Immagine (Videosorveglianza)	SI				✓					✓
Altro	NO									

L'Ente ha individuato i seguenti trattamenti basati sul **legittimo interesse:**

- **Esigenze legate alla tutela del patrimonio aziendale** mediante l'installazione di impianti di videosorveglianza.

Per questi trattamenti, l'Ente ha effettuato un bilanciamento secondo il seguente schema:

- l'Ente ha un legittimo interesse ad effettuare un tipo di Trattamento;
- il Trattamento è necessario per perseguire il proprio legittimo interesse;
- l'interesse dell'Ente non prevale sugli interessi, i diritti fondamentali e le libertà degli Interessati.

L'Ente, inoltre, ha individuato, per ciascuna categoria di Dati, in relazione a ciascuna finalità, i relativi tempi di conservazione, che ha riportato in un apposito documento (**Allegato _Data Retention policy**)

5.1.1 L'informativa

L'informativa è fornita dai Settori/Uffici di competenza prima di effettuare la raccolta dei Dati.

Informativa per i servizi ESU

L'informativa è pubblicata sul sito www.esupd.gov.it al seguente **link**
http://www.esupd.gov.it/it/Pagine/privacy.aspx

5.1.2 I *cookie*

I *cookie* sono dei file utilizzati dai *server* per poter riconoscere i browser durante comunicazioni con il protocollo HTTP usato per la navigazione *web*. Tale riconoscimento permette di: realizzare meccanismi di autenticazione, usati ad esempio per i *login*; memorizzare dati utili alla sessione di navigazione, come le preferenze sull'aspetto grafico o linguistico del sito; associare dati memorizzati dal *server o* tracciare la navigazione dell'utente, ad esempio per fini statistici.

Secondo quanto emerso nella fase di *Risk Assessment*, durante la navigazione del sito *web* dell'Ente vengono acquisiti i seguenti tipi di *cookies*:

- tecnici o analitici prima parte ;
- di terze parti.

Gli utenti del sito devono essere informati con un linguaggio chiaro e semplice in merito a chi riceve i loro dati e come sono usati, come previsto nella relativa informativa *cookie*.

I *cookie* devono essere trattati come Dati Personali e pertanto non possono essere tracciati o usati prima che l'utente abbia fornito un consenso esplicito. È necessario altresì mantenere traccia di ogni eventuale consenso al trattamento dei *cookies*.

Per ulteriori informazioni si rimanda al seguente link http://www.esupd.gov.it/it/Pagine/cookies.aspx

5.1.3 I diritti degli Studenti e Ospiti

Per la gestione dei diritti che gli Studenti e Ospiti possono esercitare nei confronti del Titolare, quest'ultimo si è dotato di una specifica procedura denominata Subject Access Request Policy (cd. **SAR Policy**).

Allegato: SAR Policy

5.2 Trattamento nei confronti di Dipendenti, Collaboratori e Candidati

L'Ente tratta i seguenti Dati Personali dei propri Dipendenti e Collaboratori:

		DIPENDENTI/COLLABORATORI								
Dati Trattati		Finalità					Base giuridica			
		Garantire il diritto allo studio	Fornire i servizi	Esecuzione del contratto	Tutela del Patrimonio	Obblighi Normativi	Interesse Pubblico	Contratto	Obbligo Legale	Legittimo interesse
Anagrafici	SI			✓		✓		✓	✓	
Di Contatto	SI			✓		✓		✓	✓	
Relativi alla salute	SI			✓		✓		✓	✓	
Condizione Economica	NO			✓		✓		✓	✓	
Di Geolocalizzazione	NO									
Biometrici	NO									
Genetici	NO									
Relativi a condanne penali e reati	NO			✓		✓		✓	✓	
Bancari	SI			✓				✓		
Status di Studente e percorso accademico	NO	✓		✓		✓			✓	
Immagine (Videosorveglianza)	SI				✓					✓
Altro	NO									

L'Ente tratta i seguenti Dati Personali dei Candidati:

	CANDIDATI								
Dati Trattati	Finalità					Base giuridica			
	Garantire il diritto allo studio	Fornire i servizi	Esecuzione del contratto	Tutela del Patrimonio	Obblighi Normativi	Interesse Pubblico	Contratto	Obbligo Legale	Legittimo interesse

Anagrafici	SI					✓			✓	
Di Contatto	SI					✓			✓	
Relativi alla salute	NO					✓			✓	
Condizione Economica	NO									
Di Geolocalizzazione	NO									
Biometrici	NO									
Genetici	NO									
Relativi a condanne penali e reati	NO					✓			✓	
Bancari	NO									
Status di Studente e percorso accademico	NO					✓			✓	
Immagine (Videosorveglianza)	SI				✓					✓
Altro	NO									

L'Ente ha individuato i seguenti trattamenti basati sul **legittimo interesse:**

- **Esigenze legate alla tutela del patrimonio aziendale** mediante l'installazione di impianti di videosorveglianza.

Per questi trattamenti, l'Ente ha effettuato un bilanciamento secondo il seguente schema:

- L'Ente ha un legittimo interesse ad effettuare un tipo di Trattamento;
- il Trattamento è necessario per perseguire il proprio legittimo interesse;
- l'interesse dell'Ente non prevale sugli interessi, i diritti fondamentali e le libertà degli Interessati.

L'Ente, inoltre, ha individuato, per ciascuna categoria di Dati, in relazione a ciascuna finalità, i relativi tempi di conservazione, che ha riportato in un apposito documento (**Allegato _Linee guida Data retention policy**).

5.2.1 L'Informativa Candidati

Il Trattamento dei candidati è effettuato dall'Ente per finalità connesse o strumentali allo svolgimento dell'attività di ricerca e selezione del personale che si svolge mediante bando pubblico.

L'informativa destinata ai candidati è resa dal Referente Privacy HR ed è parte integrante della documentazione del bando (**Allegato: Informativa candidati**).

Le informative verranno firmate dall'Interessato, per presa visione e il Referente Privacy HR è tenuto agli obblighi di conservazione della documentazione, previsti tra i compiti attribuiti in qualità di Referente.

5.2.2 L'Informativa Dipendenti e Collaboratori

L'Ente tratta Dati Personali dei Dipendenti e Collaboratori, quali, ad esempio, dati anagrafici, codice fiscale, dati retributivi, eventuali coordinate bancarie. Può accadere inoltre che, nell'adempimento di specifici obblighi relativi alla gestione del rapporto di lavoro/collaborazione (nei limiti in cui sia applicabile), l'Ente venga in possesso di Categorie particolari di dati e cioè quelli da cui possono eventualmente desumersi, fra l'altro, l'origine razziale ed etnica, l'adesione a partiti, sindacati, nonché un generale stato di salute (ad esempio, certificati di malattia e infortunio; certificati di gravidanza; appartenenza alle c.d. categorie protette; esiti di visite mediche effettuate ai sensi di legge e di contratto, *etc.*).

Allegato: Informativa Dipendenti e Collaboratori

Le informative verranno firmate dall'Interessato, per presa visione e il Referente Privacy HR è tenuto agli obblighi di conservazione della documentazione, previsti tra i compiti attribuiti in qualità di Referente.

5.2.3 Il consenso

L'Ente richiede il consenso dei Dipendenti qualora sia necessario trattare le immagini degli stessi, per inserimento nell'organigramma, sulla intranet aziendale o in altri documenti aziendali. Il Referente Privacy HR raccoglierà, su supporto cartaceo, i consensi dei Dipendenti archiviandoli nei fascicoli del personale, ai fini di permettere in qualsiasi momento le opportune verifiche.

5.2.4 Il Regolamento per l'utilizzo degli strumenti aziendali

L'Ente ha adottato con decreto del Direttore il Regolamento per l'utilizzo degli strumenti aziendali avente ad oggetto la regolamentazione dell'utilizzo degli strumenti aziendali con cui il Personale svolge le attività per conto del Titolare (PC, TABLET, smartphone aziendali, rete internet ed intranet, posta elettronica aziendale, …). In relazione ai Dipendenti, in particolare, il Regolamento è informato al principio dall'art. 4 comma 3 della L. 300/1970 (Statuto dei Lavoratori), secondo cui le informazioni raccolte tramite gli strumenti adoperati dal lavoratore per rendere la prestazione lavorativa e quelli necessari alla registrazione degli accessi e delle presenze, possono essere utilizzate ai fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione sulle modalità d'uso degli strumenti utilizzati e di effettuazione dei controlli, nel rispetto di quanto disposto dalla Normativa Vigente.

Si allega il **link dove è consultabile il regolamento**: https://esupd.e-pal.it/L190/atto/show/102709?

5.2.5 I diritti dei Dipendenti

Il Dipendente può esercitare nei confronti del Titolare i diritti riconosciuti dal GDPR. Le relative richieste del Dipendente devono essere indirizzate al Referente Privacy HR che deve provvedere al tempestivo riscontro ed all'evasione entro 30 giorni dalla corretta ricezione della richiesta stessa. A tale proposito Il Titolare si è dotato di una specifica procedura denominata Subject Access Request Policy (**Allegato_ SAR Policy**).

5.3 I Terzi

Per Terzi l'Ente intende:

- Fornitori ;

- Stakeholders ;
- Membri del CdA ;

L'Ente tratta i seguenti Dati Personali di Terzi:

		TERZI								
Dati Trattati		Finalità					Base giuridica			
		Garantire il diritto allo studio	Fornire i servizi	Esecuzione del contratto	Tutela del Patrimonio	Obblighi Normativi	Interesse Pubblico	Contratto	Obbligo Legale	Legittimo interesse
Anagrafici	SI			✓		✓		✓	✓	
Di Contatto	SI			✓		✓		✓	✓	
Relativi alla salute	NO									
Condizione Economica	NO									
Di Geolocalizzazione	NO									
Biometrici	NO									
Genetici	NO									
Relativi a condanne penali e reati	SI					✓			✓	
Bancari	SI			✓				✓		
Status di Studente e percorso accademico	NO									
Immagine (Videosorveglianza)	SI				✓					✓
Altro	NO									

L'Ente ha individuato i seguenti trattamenti basati sul **legittimo interesse**.

- **Esigenze legate alla tutela del patrimonio aziendale** mediante l'installazione di impianti di videosorveglianza.

Per i trattamenti basati su un legittimo interesse, l'Ente ha effettuato un bilanciamento secondo il seguente schema:

- L'Ente ha un legittimo interesse ad effettuare un tipo di Trattamento;
- il Trattamento è necessario per perseguire il proprio legittimo interesse;
- l'interesse dell'Ente non prevale sugli interessi, i diritti fondamentali e le libertà degli Interessati.

L'Ente, inoltre, ha individuato, per ciascuna categoria di Dati, in relazione a ciascuna finalità, i relativi tempi di conservazione, che hanno riportato in un apposito documento (**Allegato _*Linee Guida data retention policy*)**.

5.3.1. L'Informativa

L'informativa sarà messa a disposizione del Terzo qualora entri in contatto con ESU. I Dati dei Terzi vengono trattati per finalità strettamente connesse e strumentali alla gestione del rapporto con l'Ente, nonché per le finalità previste da leggi, da regolamenti e dalla normativa comunitaria.
Allegato: Informativa Terzi

5.3.2 I diritti dei Terzi

Per la gestione dei diritti che i Terzi possono esercitare nei confronti del Titolare, quest'ultimo si è dotato di una specifica procedura denominata Subject Access Request Policy (cd. SAR Policy).
Allegato: SAR Policy

6. Gli strumenti di trattamento

6.1 Il Registro delle attività di trattamento del Titolare

L'articolo 30 del GDPR prevede che ogni Titolare debba tenere un registro delle attività di Trattamento. Sono esentate dalla tenuta del Registro le imprese od organizzazioni con meno di 250 Dipendenti, a meno che il trattamento effettuato:

- possa presentare un rischio per i diritti e le libertà degli Interessati;
- il trattamento non sia occasionale;
- includa il trattamento di categorie particolari di dati;

L'Ente in qualità di Titolare ha predisposto e mantiene il proprio Registro disponibile presso il Gruppo di Lavoro GDPR.

6.2 *Data Breach*

Secondo quanto previsto dal GDPR, in caso di violazione dei Dati Personali, l'Ente deve notificare al Garante la relativa violazione senza ritardo, a meno che sia improbabile che la violazione dei Dati Personali presenti un rischio per i diritti e le libertà degli Interessati.

Ciò avviene quando il *Data Breach* comporti l'insorgenza o l'aggravamento di danni, quali perdita del controllo dei propri Dati Personali, discriminazione, furto o usurpazione di identità, perdite finanziarie, decifratura non autorizzata della pseudo-anonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei Dati Personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo.

Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà degli Interessati, l'Ente deve altresì – salvo alcune specifiche e circoscritte eccezioni – darne comunicazione agli Interessati stessi.

Gli obblighi di comunicazione descritti sopra devono essere effettuati nel rispetto di precise tempistiche e contenuti formali e prevedono, altresì, alcune valutazioni preliminari che devono accompagnare sia la fase

dell'individuazione dell'esistenza o meno di un reale *Data Breach*, sia la valutazione sulla necessità di procedere alla notificazione al Garante ovvero alla comunicazione agli Interessati.

I processi per la gestione del Data Breach sono normati secondo l'allegato di cui al DD n. 330/2019 consultabile al seguente **link** https://esupd.e-pal.it/L190/atto/show/102709?

6.3 *Data Protection Impact Assessment* (DPIA)

In conformità all'articolo 35 del GDPR, l'Ente procede ad una DPIA in fase di sviluppo di ogni nuova iniziativa o servizio previsto, o di nuovi applicativi e soluzioni informatiche, in particolare qualora il nuovo Trattamento sia caratterizzato da almeno due dei seguenti elementi:

- profilazione, trattamenti valutativi e *scoring* (ad es. creazione di profili comportamentali, basati sulle scelte effettuate o sulla navigazione sul sito *web*);
- decisioni automatizzate che producono significativi effetti giuridici o di analoga natura (ad es. inclusione o esclusione automatica, senza valutazione ulteriore, di Fornitori in/da procedure di gara, sulla base dei dati forniti);
- monitoraggio sistematico (ad es. sorveglianza sistematica di aree pubbliche);
- categorie particolari di dati;
- trattamenti su larga scala (da determinare sulla base del numero di Interessati, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata, o persistenza, dell'attività di Trattamento; ambito geografico dell'attività di Trattamento);
- combinazione o raffronto di insiemi di dati (ad es. derivanti da due o più Trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'Interessato);
- dati relativi a Interessati vulnerabili (ad es. minori);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
- trattamenti che, di per sé, "impediscono [agli Interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto". Ciò comprende i trattamenti finalizzati a consentire, modificare o negare l'accesso degli Interessati a un servizio o la stipulazione di un contratto.

Per la procedura da seguire si rinvia alla lettura della Procedura per valutazione di impatto sulla protezione dei dati in caso di rischio elevato

Allegato:
Procedura DPIA (per valutazione di impatto sulla protezione dei dati in caso di rischio elevato)

7. Altri trattamenti rilevanti

7.1 Videosorveglianza

Ai sensi dell'art. 4 della L. 300/1970 (Statuto dei Lavoratori) e delle misure di tutela ivi previste, sono installate presso le sedi dell'Ente delle telecamere unicamente per esigenze di tutela del patrimonio aziendale.

Per il rispetto della normativa e di alcuni degli adempimenti richiesti dalla normativa in materia di protezione dei Dati Personali la presenza degli impianti è segnalata da una specifica informativa collocata presso la reception e da un'informativa sintetica situata nelle vicinanze di ogni telecamera.

8. La Governance IT

8.1 I principi del GDPR

Il GDPR "rifonda" le misure minime di sicurezza alla base del sistema di protezione dei dati personali, modificando radicalmente approccio e lasciando al Titolare ampio margine di libertà di scelta in funzione della realtà produttiva nella quale opera.

Questo nuovo sistema poggia i cardini su tre principi fondamentali:

- la necessità di un'analisi del rischio;
- la stretta connessione con la migliore tecnica e i costi da supportare;
- la comprensione e l'applicazione costante della nozione di "accountability".

L'ente, come già evidenziato, per garantire il rispetto dei suddetti principi ha condotto un'attività di Risk Assessment, all'esito della quale ha deciso di dotarsi di un Documento per la valutazione dei rischi che riassume, per poi rinviare alle policy IT di dettaglio, le misure di sicurezza adottate per contenere il rischio di *data incident,* come riportato nel decreto del Direttore n. 6 del 08.01.2019.