AVV. LAURA PISCINI
STUDIO LEGALE

OGGETTO: Relazione in ordine all'adeguamento dell'Istituto al Regolamento generale sulla protezione dei dati n. 679/2016 (General Data Protection Regulation - GDPR).

-1-
Inquadramento della normativa

1.1 Premessa.

Il Reg. (UE) n. 679 del 2016 emanato dal Parlamento Europeo e dal Consiglio il 27 aprile 2016 è stato pubblicato in data 4 maggio 2016 nella Gazzetta ufficiale dell'Unione Europea.
Tale Regolamento si occupa della «*protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*», si articola in 11 capi per un totale di 99 articoli.
Il GDPR, acronimo di General Data Protection Regulation (Regolamento Generale sulla Protezione dei Dati) abroga e sostituisce la direttiva 95/46/CE.
La nuova normativa europea nasce dall'esigenza di uniformare la disciplina di settore all'interno dell'Unione Europea e, nel contempo, di fare fronte alla continua evoluzione degli stessi concetti di privacy e di *data protection*, dovuta anche al progresso dei servizi *on line*.

1.2 Ambito di applicazione del regolamento.

Il Regolamento in esame si applica a qualsiasi forma di trattamento di dati personali siano essi automatizzati o contenuti in un archivio (art. 2 comma 1 Reg. UE 679/2016).
Il regolamento non si applica ai trattamenti di dati personali:
a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, Testo Unico dell'Unione Europea (si tratta delle disposizioni specifiche sulla politica estera e di sicurezza comune);
c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

1.3 Definizioni.

1.3.A. Dato personale.
In base all'art. 4 del Regolamento la definizione di "dato personale", coincide con qualsiasi informazione riguardante una persona fisica identificata o identificabile (il c.d. interessato).
I dati personali si possono distinguere in:
a-dati comuni (es anagrafici, Indirizzi postali, indirizzi IP, codici identificativi, conto corrente, carta di credito ecc..);

b-dati particolari o ex sensibili (origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, stato di salute, orientamento/vita sessuale ecc..)
c-dati penali (condanne penali, reati, misure di sicurezza)
d-dati che presentano rischi o quasi sensibili perché presentano rischi elevati per la libertà /dignità della persona (profilazione es rendimento professionale/scolastico, trattamenti su larga scala, geolocalizzazione, videosorveglianza....)
e-dati genetici, relativi alle caratteristiche genetiche - ereditarie o acquisite - di una persona fisica, che forniscono informazioni univoche sulla sua fisiologia o sulla sua salute e che risultano in particolare dall'analisi di un campione biologico;
f-dati biometrici, 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.

1.3.B Trattamento.

Il "trattamento" è definito come qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o a insiemi di dati personali. Pertanto, costituiscono trattamento di dati personali la relativa 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.

1.3.C Titolare e responsabile trattamento.

Il punto 4 dell'art. 4 definisce il «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Il punto 8 definisce, invece, il «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

-2-

Principi fondamentali ispiratori del Regolamento

I principi fondamentali contenuti nella disciplina del Regolamento n.679/2018 sono i seguenti:

- liceità del trattamento;
- trasparenza nel trattamento;

- diritto all'oblio;
- "accountability" (una sorta di commistione tra responsabilità e rispetto di norme regolamentari) del titolare del trattamento;
- *privacy by design e by default.*

2.1 Liceità del trattamento.

Il principio di liceità del trattamento in base all'art. 6 del regolamento, presuppone l'esistenza di due requisiti alternativi:

- la necessità del trattamento
- il consenso dell'interessato.

In altri termini, il trattamento è lecito quando si tratta di operazione necessaria o quando c'è il consenso dell'interessato - da esprimersi in relazione ad «*una o più specifiche finalità*», e dunque non genericamente.

I casi di necessità sulla scorta dell'art. 6 sono individuabili:

- nel caso di trattamento «necessario all'esecuzione di un contratto di cui l'interessato è parte»,
- o di trattamento «necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica» (come, ad esempio, le emergenze cliniche)
- nel caso di trattamento «necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento» (si pensi, ad esempio, al trattamento che il notaio deve fare dei dati personali dei suoi clienti, al fine di dar corso alla pubblicità immobiliare di un suo atto, cui egli è tenuto per legge a dar corso).

L'art. 4 definisce, poi, il requisito del consenso, che rappresenta il parametro di liceità del trattamento quante volte questo non sia connotato dal carattere della necessità. Costituisce "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

L'art. 7 disciplina il consenso articolandolo in un fase precedente al rilascio dello stesso e ad una fase successiva, dell'eventuale revoca.

Quanto alla prima fase, il regolamento stabilisce che, «*il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro*».

L'art. 7 dispone, altresì, che «*nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante*». In altre parole, nel caso in cui la dichiarazione scritta di contenuto complesso integri una violazione del regolamento, essa è inefficace. È inoltre previsto sempre dall'art. 7 che l'interessato debba essere informato, prima di esprimere il consenso, della facoltà di revocarlo in seguito, senza pregiudizio della liceità

del trattamento effettuato prima della revoca.

2.2 Trasparenza.

Il principio di trasparenza, in base all'art. 12 del Regolamento riguarda il rapporto fra il titolare del trattamento e l'interessato con riferimento all'informazione e all'accesso ai dati.

Il rispetto di tale principio viene perseguito con l'adozione di modalità informative e seguendo un modello di gestione. È previsto che le informazioni destinate al pubblico o all'interessato debbano essere facilmente accessibili e di facile comprensione, ed espresse con linguaggio semplice e chiaro. Ciò riguarda in particolare l'informazione degli interessati circa l'identità del titolare del trattamento e le finalità del trattamento, nonché le ulteriori informazioni relative al diritto degli interessati di ottenere conferma e comunicazione del trattamento di dati personali che li riguardano.

2.3 Il diritto all'oblio.

L'art. 17 del regolamento stabilisce che «*l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali*». Il "diritto all'oblio" può verificarsi in situazioni di natura obbiettiva e altre di natura soggettiva: fra le prime si registrano quelle in cui i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti; quella in cui i dati personali sono stati trattati illecitamente e quella in cui i dati personali devono essere cancellati per adempiere un obbligo legale; fra le situazioni soggettive vi sono quelle in cui l'interessato revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per il trattamento (vale a dire la necessità dello stesso), nonché quella in cui l'interessato si oppone al trattamento.

2.4 Principio di *accountability*.

L'art. 24 del Regolamento prevede che "*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, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.*

Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento".

Sulla base di tale norma si può afferma che "l'accountability" dev'essere intesa non già come

completa accessibilità, da parte dell'interessato, alle informazioni circa l'attività di un dato operatore, bensì come garanzia della conformità di tale attività alla disciplina di settore: conformità che l'operatore - il titolare del trattamento - dev'essere in grado di dimostrare in qualsiasi momento.

Da questo punto di vista, una sorta di facilitazione deriva dall'adesione del titolare del trattamento a un codice di condotta: così dispone l'art. 243, il quale afferma che «*l'adesione ai codici di condotta (...) o a un meccanismo di certificazione (...) può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento*». Al di là del piano probatorio, sembra comunque che il principio di *accountability* imponga ai titolari del trattamento, ai fini della sua attuazione, l'adozione di «un sistema di controllo della protezione dei dati, strutturato in base a standard di buona amministrazione riconosciuti universalmente e che sia verificabile (auditable) all'esterno, in quanto il rispetto delle regole in materia di dati personali da parte dei titolari del trattamento dei dati richiede non il mero adempimento delle disposizioni di legge ma la predisposizione di una vera e propria governance interna.

2.5 Principio di *privacy by design e by default*

L'art. 25 del regolamento, rubricato come "*Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita*" prevede quanto segue: «*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 del trattamento 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, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. Il titolare del trattamento 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 l'intervento della persona fisica. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo*».

In sostanza il principio della ***privacy by design*** implica che la protezione dei dati sia integrata nell'intero ciclo di vita di una data tecnologia o servizio o processo, sin dalla relativa

progettazione: in altre parole, qualsiasi progetto deve essere realizzato avendo presente, sin dal principio - by design, appunto - la riservatezza dell'utente finale e la protezione dei suoi dati personali, con tutte le necessarie applicazioni di supporto (informatiche e non). Si tratta di un approccio sempre più utilizzato al problema della protezione dei dati, volto a garantire la migliore operatività possibile della protezione.

Il principio della ***privacy by default*** implica che i dati vengano raccolti nella minore misura possibile e che le finalità del trattamento siano quanto più possibile limitate. Si tratta, in altre parole, della summa dei principi di "minimizzazione dei dati" e di "limitazione della finalità" (da cui discende a sua volta il principio della "limitazione della conservazione", il quale impone di limitare nel tempo quanto più possibile il trattamento e l'archiviazione dei dati raccolti).

-3-

Profili di responsabilità.

L'art. 82 del regolamento prevede che "*chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.*

Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile".

L'art. 83 del regolamento prevede sanzioni amministrative nei confronti del titolare del trattamento "*1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.*

2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

b) il carattere doloso o colposo della violazione;

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;
e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
g) le categorie di dati personali interessate dalla violazione;
h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e
k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione".
Con l'attuazione del modello di gestione di protezione dei dati personali, conforme alle previsioni del Regolamento 679/16 ed il rispetto dello stesso, viene a precostituirsi la formazione di una sorta di prova liberatoria da profili di responsabilità in relazione al mancato rispetto del Regolamento stesso.

-4-

Aspetti operativi nelle attività di trattamento dei dati personali

4.1 Registro del trattamento.

L'art. 30 del Regolamento ha introdotto il registro delle attività di trattamento. Tale norma, in particolare, prevede che "*ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:*
a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, 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 i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:
a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) ove applicabile, 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 i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.
4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.
5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10".
Sulla base di tale norma si possono sintetizzare nei termini che seguono i contenuti dei due registri.

Registro del titolare	Registro del responsabile[1]
a) nome e dati di contatto del titolare e, ove applicabile, del rappresentante e del titolare e del responsabile della protezione dei dati	*a) nome e dati di contatto del responsabile, di ogni titolare per cui esso agisce, del rappresentante del titolare o del responsabile e, ove applicabile, del responsabile della protezione dei dati*
b) finalità del trattamento	**b) categorie dei trattamenti effettuati per conto di ogni titolare**
c) categorie di interessati e di dati personali	*(ove applicabile), trasferimenti di dati verso un Paese extra-UE o un'organizzazione internazionale e, per i trasferimenti di cui all'art. 49, par. 2, la documentazione delle garanzie adeguate*
d) categorie di destinatari (compresi quelli di Paesi extra-UE e le organizzazioni internazionali)	*d) (ove possibile), descrizione generale delle misure di sicurezza, tecniche e organizzative di cui all'art. 32, par. 1*
e) (ove applicabile) trasferimenti di dati verso Paesi extra-UE e/o organizzazioni internazionali e, per i trasferimenti di cui all'art. 49, par. 2, la documentazione delle garanzie adeguate	
f) (ove possibile) termini ultimi di cancellazione delle diverse categorie di dati	
g) (ove possibile) descrizione generale delle misure di sicurezza, tecniche e organizzative di cui all'art. 32, par. 1.	

4.2 Misure di sicurezza.

L'art. 32 del regolamento prevede che "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione[2] e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

4.3 Valutazione d'impatto.

L'articolo 35 del regolamento introduce il concetto di valutazione d'impatto sulla protezione dei dati (il Gruppo di Lavoro di cui all'art. 29 del Regolamento in data 4 ottobre 2017 ha adottato le Linee Guida n. WP248).
Si tratta di un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento. In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità.

4.4 Nomina DPO (Data Protection Officer) o RPD (Responsabile della protezione Dati.

Il DPO è una sorta di consulente esperto, previsto dagli artt. 38 e 39 del Regolamento che affianca il titolare nella gestione delle problematiche del trattamento dei dati personali; in tal modo si garantisce che un soggetto qualificato si occupi in maniera esclusiva della materia della protezione dei dati personali, aggiornandosi sui rischi e le misure di sicurezza, in considerazione della crescente importanza e complessità del settore.
In base all'art. 39 del Regolamento il DPO è tenuto:
- ad informare e fornire consulenza al titolare e al responsabile del trattamento in merito agli obblighi derivanti dal Regolamento 679/2016 o dalle altre disposizioni legislative interne o europee in materia di protezione dati;
- a sorvegliare l'osservanza del Regolamento da parte del titolare e del responsabile del trattamento in tutte le sue parti, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa al trattamento;
- a fornire su richiesta pareri in merito alla valutazione d'impatto e sorvegliarne lo svolgimento;
- a cooperare con l'autorità di controllo fungendo, tra le altre cose, da punto di contatto per

[2] La pseudonimizzazione è una tecnica che consiste nel conservare i dati in una forma che impedisce l'identificazione del soggetto senza l'utilizzo di informazioni aggiuntive, che sono detenute separatamente

questioni connesse al trattamento effettuando consultazioni di ogni tipo, con particolare riguardo e attenzione ad un'eventuale attività di consultazione preventiva.

-5-

Considerazioni conclusive

L'adozione di un modello di gestione dei dati personali in conformità al Regolamento 679/2016 si pone in linea con la politica dell'istituto volta al rispetto dei principi di liceità, trasparenza, correttezza e di tutela della riservatezza e dei diritti.

Il modello GDPR, quindi, arricchisce i processi gestionali. Nell'ottica di un efficace Modello GDPR si deve tenere conto della struttura dell'Istituto e del numero di personale occupato tra dipendenti e collaboratori, e provvedere ad :

- individuare le figure responsabili secondo il Regolamento: titolare del trattamento, responsabile del trattamento (individuato in relazione alla specifica area di attività), incaricato dal responsabile del trattamento;
- redigere il registro del trattamento sia da parte del titolare che da parte dei responsabili (sia interni che esterni) del trattamento dei dati;
- curare la formazione dei soggetti che trattano i dati personali;
- nominare il DPO quale organo consulente e di controllo;
- seguire protocolli informativi nei confronti degli interessati (es.studenti/utenti, fornitori, dipendenti) attraverso modelli recanti tutte le informazioni necessarie affinché vi sia il consenso informato al trattamento dei dati;
- predisporre idonee misure di sicurezza con particolare riguardo ai processi informatizzati in linea con quanto previsto dall'art. 32 del Regolamento;
- elaborare un documento di valutazione d'impatto secondo l'impostazione delle Linee Guida del 4.10.2017 del Gruppo di Lavoro.

***

Si resta a disposizione per ogni necessità ed integrazione.

Cordiali saluti