Relazione del Responsabile della Protezione dei Dati

Anno 2021

Camerino, gennaio 2022

INDICE

Introduzione.

Un utilizzo corretto dei dati personali e il riconoscimento del potere di controllo sugli stessi in capo alla persona fisica a cui si riferiscono assumono oggi crescente importanza nell'ambito della Pubblica Amministrazione, ponendo l'esigenza di trovare un giusto contemperamento con l'esercizio delle funzioni svolte nell'interesse della collettività.

Unicam si è prontamente adeguata alle previsioni normative che impongono l'istituzione del Responsabile della Protezione dei Dati (RPD)[1]; attualmente questa figura è stata identificata con Responsabile del Gruppo di Supporto Anticorruzione, Trasparenza e Privacy, che per la natura della funzione a cui è preposto, mantiene un rapporto di terzietà con tutte le attività e le strutture dell'Ateneo.

Il RPD svolge in autonomia un ruolo di confronto dialettico con gli uffici/aree amministrative, le strutture e, in particolare, con il Titolare del trattamento dei dati, che in Unicam è il Rettore, e con il Direttore Generale, al vertice della gestione amministrativa dell'Ateneo.

L'anno 2021, pur nelle condizioni definite dalle normative preordinate al contenimento del rischio epidemico, ha fatto registrare un consolidamento delle attività del RPD, con un ampliamento dei contatti con le strutture per consultazioni su questioni di *privacy* e per consulenze sulle valutazioni di impatto dei trattamenti di dati collegati a nuovi progetti o procedure e sui casi di potenziale *data breach*.

Si sono moltiplicate le occasioni di confronto e di raccordo con le funzioni di protezione dei dati operanti all'interno delle strutture per l'espressione di opinioni o posizioni comuni sulla *compliance* con il GDPR di trattamenti di dati condivisi o collegati effettuati dalle diverse aree.

Crescente è il ruolo di coordinamento assunto dal Gruppo di Lavoro del CODAU che si occupa di questi temi nei confronti dei RPD degli Atenei, in particolar modo sull'applicazione di norme e linee guida, nella promozione di accordi per disciplinare i casi di contitolarità dei trattamenti di dati e nella sollecitazione di iniziative comuni.

Pur non essendo un obbligo stabilito dalla normativa, la presente Relazione, la prima per l'Università degli Studi di Camerino, rientra in quelle attività di condivisione tra RPD e governance di Ateneo.

1. Il quadro giuridico e l'organizzazione interna.

La normativa in materia di protezione dei dati è mutata sotto molteplici aspetti a seguito dell'entrata in vigore del Regolamento UE 679/2016 e della modifica del d.lgs. 196/2003 ad opera del d.lgs. 101/2018. Una delle novità di maggior rilievo riguarda la definizione dei ruoli, dei compiti e delle responsabilità di coloro che trattano dati personali. La chiave di lettura che

[1] Regolamento UE 2016/679 (GDPR). Le funzioni del RPD, definite nell'art. 39 del GDPR, si distinguono in compiti di consulenza, di sorveglianza in materia di protezione dei dati e di collegamento con il Garante per la protezione dei dati personali (Garante *privacy*), autorità di controllo nazionale in materia ex art. 51 GDPR.

guida la riforma in tal senso è il ***principio di accountability***, secondo il quale spetta al Titolare definire l'organizzazione che meglio si adatta alle specifiche peculiarità dell'ente medesimo. La normativa, pertanto, si limita a definire alcuni ruoli chiave e a definirne le principali attribuzioni, rimettendo, poi, al Titolare la definizione delle misure organizzative pertinenti all'organizzazione che presiede.

La normativa europea mantiene la figura del ***Titolare del trattamento*** (art. 4, n. 7 GDPR), che è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che decide i mezzi e le finalità del trattamento dei dati personali, ma mutano altri ruoli interni ed esterni all'organizzazione.

Si introduce, quindi, la figura del ***Contitolare del trattamento*** (art. 26 GDPR), che è colui con cui il Titolare condivide il proprio potere decisionale in merito a finalità e mezzi del trattamento stesso. In tali circostanze i Contitolari definiscono in modo trasparente, mediante accordo interno, le rispettive responsabilità in merito agli obblighi nascenti dalla normativa vigente.

Altra figura cardine è quella del ***Responsabile del trattamento*** (artt. 4 e 28 GDPR) è colui che tratta i dati personali per conto del Titolare, distinguendosi, pertanto, da quest'ultimo in quanto esterno alla sua organizzazione. Egli può essere una persona fisica o giuridica, autorità pubblica, servizio o altro organismo, purché presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti posti dalla normativa. Il Regolamento pone in carico del Responsabile specifiche responsabilità in caso di violazione della normativa in materia o delle istruzioni del Titolare.

Laddove, inoltre, specifiche attività di trattamento siano svolte da una diversa e ulteriore persona fisica o giuridica per conto del Responsabile del trattamento, previa autorizzazione scritta generica o specifica del Titolare, la normativa prevede l'individuazione del ***Sub-responsabile del Trattamento*** (artt. 4 e 28 GDPR). Quest'ultimo è tenuto a rispettare i medesimi obblighi in materia di protezione dei dati personali contenuti nel contratto o nell'altro atto giuridico stipulato tra il Titolare e il Responsabile.

Diverso ruolo è quello del ***Designato*** (art.2-quaterdecies, comma 1, D. Lgs. 196/2003, come modificato dal D.lgs. 101/2018), che è la persona fisica che opera internamente all'organizzazione e sotto l'autorità del Titolare (o del Responsabile) e a cui questi attribuisce specifici compiti e funzioni connessi al trattamento di dati personali.

A fianco di tali figure il Regolamento Eu introduce ex novo il ruolo di ***Responsabile della Protezione dei Dati (RPD/DPO)*** (artt.37-39 GDPR), il quale, tra le altre attività, fornisce consulenza al Titolare e al personale di questi, vigila sull'osservanza del Regolamento e funge da punto di contatto con il Garante della Privacy e con gli interessati. Egli svolge la sua attività in autonomia e senza ricevere alcuna istruzione per l'esecuzione dei compiti che gli sono attribuiti.

Con la Disposizione del Direttore Generale n. 11236 del 22 febbraio 2021 è stato costituito all'interno di Unicam il nuovo Gruppo di Supporto Anticorruzione, Trasparenza e Privacy composto da:

- Stefano Burotti (Responsabile Protezione Dati) – Responsabile del Gruppo;
- Sara Buti (Area Infrastrutture, Servizi informatici e Amministrazione digitale);
- Claudia Caprodossi (Area Persone, Organizzazione e Sviluppo);
- Alessandra Ciccarelli (Avvocatura di Ateneo);
- Francesco De Angelis (Area Infrastrutture, Servizi informatici e Amministrazione digitale);
- Giulia Giontella (Avvocatura di Ateneo);
- Cecilia Mancia (Area Affari Legali);
- Andrea Orlando (Area Infrastrutture, Servizi informatici e Amministrazione digitale);

Il Gruppo collabora con il Responsabile della Protezione Dati, supportando lo stesso negli adempimenti assegnati con Decreto Rettorale Prot. n. 37098 del 24/06/2020:
a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del RGPD, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del RGPD;
d) cooperare con il Garante per la protezione dei dati personali;
e) fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Il Codice nazionale in materia di protezione dei dati personali (Codice privacy), già integralmente rivisto per l'adeguamento al GDPR, è stato recentemente modificato dal decreto-legge 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla legge 3 dicembre 2021, n. 205 e dal decreto-legge 30 settembre 2021, n. 132, convertito, con modificazioni, dalla legge 23 novembre 2021, n. 178.

Il trattamento dei dati personali viene effettuato dall'Università degli Studi di Camerino per lo svolgimento di funzioni istituzionali (e, pertanto, ai sensi dell'art. 6 comma 1 lett. e), non necessita del consenso dell'interessato, o per eseguire richieste degli stessi interessati (in tal caso, i dati personali forniti dagli utenti che inoltrano richieste di invio di materiale informativo quali newsletter, documenti, risposte a quesiti, ecc., sono utilizzati al solo fine di eseguire il servizio o la prestazione richiesta e sono comunicati a terzi nel solo caso in cui ciò sia a tal fine necessario), per eventuale adempimento di obblighi legali che ricadono sull'Ateneo, per lo svolgimento di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri di cui è investita l'Università degli Studi di Camerino, o laddove sia stato prestato un consenso libero, specifico e informato, ed infine laddove sia necessario per adempiere a un ordine dell'autorità giudiziaria o richieste delle forze di Polizia.

La disciplina dei trasferimenti di dati personali extra UE assume particolare rilevanza per

quanto riguarda alcuni progetti di ricerca, anche a seguito dell'uscita del Regno Unito dall'Unione Europea. L'Accordo commerciale e di cooperazione stipulato il 30 dicembre 2020 fra Regno Unito e Unione Europea prevedava che il Regno Unito continui ad applicare il GDPR per un periodo transitorio di 6 mesi nel quale qualsiasi comunicazione di dati personali verso il Regno Unito può avvenire secondo le medesime regole valevoli fino al 31 dicembre 2020 senza essere considerata un trasferimento di dati verso un Paese terzo.

2. L'attività svolta nel 2021.

Seppure con tutte le limitazioni dovute alla crisi emergenziale derivante dal dilagare dell'epidemia da COVID-19, nel corso del 2021 si è registrato un incremento complessivo del volume di attività del RPD e del Gruppo di Supporto per quanto riguarda le attività connesse al trattamento dei dati personali; sono cresciuti gli incontri telematici con i componenti del gruppo e, in particolare, gli impegni connessi con la partecipazione alle riunioni del Gruppo di lavoro CODAU e ad altri *network* dei RPD delle Università, così come la partecipazione ai webinar promossi dal Garante per la Protezione dei Dati Personali.

Importante è stata anche l'attività complessivamente dedicata allo svolgimento di valutazione di impatto sulla protezione dei dati (DPIA), ovvero quel processo finalizzato – di norma a seguito di modifiche tecnologiche od organizzative - a riesaminare il trattamento dei dati, valutarne la necessità e la proporzionalità in termini di minimizzazione dei dati utilizzati e dei tempi di conservazione, esaminarne i rischi per i diritti e le libertà delle persone fisiche destinatarie del trattamento e determinare le misure di sicurezza per mitigarli, e l'attività di valutazione approfondita di singoli trattamenti (c.d. assessment), che di norma richiede incontri e colloqui con le strutture interessate.

Con il nuovo assetto organizzativo, la funzione del RPD ha assunto un carattere "trasversale", essendo chiamata a interloquire ad ampio raggio con diverse funzioni istituzionali e aziendali: la crescita dell'attività, soprattutto in termini qualitativi, e la complessità delle relazioni che si sono consolidate hanno giustificato pienamente l'evidenza strutturale all'operatività che supporta i compiti del Responsabile.

2.1 Il registro dei trattamenti.

Uno dei primi compiti affrontati nel corso del 2021 è stato quello di consulenza al Titolare del Trattamento per la redazione del Registro dei Trattamenti. L'art. 30 del Regolamento (EU) n. 679/2016 prevede tra gli adempimenti principali del titolare del trattamento la tenuta del registro delle attività di trattamento. È un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del RGPD) relative alle operazioni di trattamento svolte dal titolare. Costituisce quindi uno dei principali elementi di accountability del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

Per condurre questa attività si è utilizzata come base di partenza il lavoro svolto a partire dal 2017 dal Gruppo di lavoro "Linee Guida Privacy e GDPR" del CODAU (ora confluito nel

Gruppo che si occupa anche di Prevenzione della Corruzione e Trasparenza) che hanno portato alla redazione delle "Linee guida in materia di privacy e protezione dei dati personali in ambito universitario", all'interno delle quali è stata stilata una mappatura dei principali trattamenti che trovano svolgimento in ambito universitario con l'obiettivo di consentire di completare in modo più agevole il registro dei trattamenti, tenuto conto del fatto che gran parte dei dati personali e delle finalità del trattamento sono comuni a molti Atenei.

Si è proceduto, innanzitutto, prendendo in considerazione la categoria di interessati cui il trattamento è rivolto (studenti – dipendenti – trattamenti trasversali a più categorie di interessati), per poi dettagliare i singoli trattamenti in relazione alle finalità da perseguire. Infine, per ciascuna categoria di interessati e nell'ambito delle differenti finalità perseguite, sono presi in analisi i seguenti aspetti:

- **Natura dei dati** L'analisi sulla natura dei dati consente di determinare se, e in quale misura, possono essere trattati (come ad esempio: categorie particolari di dati personali di cui all''art. 9 e/o i dati relativi a condanne penali e reati di cui all'art. 10), evidenziando eventuali accorgimenti adottati da alcuni Atenei nel trattamento di tali dati.
- **Quali sono i dati personali strettamente necessari per perseguire la finalità descritta** L'analisi sui tipi di dati che sono strettamente necessari per perseguire un obbligo legale o di quelli strettamente connessi all'esecuzione di compiti istituzionali favorisce la definizione di tempi di conservazione differenti o la previsione di differenti garanzie per l'interessato.
- **Modalità per fornire l'informativa e, ove necessario, acquisire il consenso** Tenuto conto del nuovo GDPR, nonché dell'obbligo di indicare nell'informativa "la base giuridica del trattamento" e "i legittimi interessi perseguiti dal titolare del trattamento" si ritiene opportuno fornire all'interessato maggiori dettagli sulle finalità. Sono quindi condivise anche alcune valutazioni in merito all'opportunità di raccogliere un consenso ad hoc per le diverse finalità non connesse a obblighi legali o allo svolgimento di compiti strettamente istituzionali.
- **Archiviazione e conservazione (tempi, modi, quali dati)** L'informativa sulla privacy dovrà indicare il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo. Tale informazione è utile anche nell'ambito della redazione dei registri di trattamento: sarà infatti importante determinare i termini ultimi previsti per la cancellazione delle diverse categorie di dati. I trattamenti possono essere compiuti con o senza l'ausilio di processi automatizzati.
- **Diritti dell'interessato**
- **Categorie di interessati** Le categorie di persone fisiche cui si riferiscono i dati personali. Ad esempio: studenti, personale dipendente, collaboratori, fornitori, ospiti.
- **Categorie di destinatari** È previsto individuare nell'informativa le categorie di destinatari a cui i dati personali possono essere comunicati. Si dovrà quindi dare indicazione di tutte le persone che possono ricevere comunicazione di dati personali (es: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che possono venire a conoscenza dei dati, nonché, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali).

- **Comunicazione e trasferimento all'estero** Occorre chiarire nell'informativa l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale. Tale dato è rilevante anche nell'ambito della redazione del registro, pertanto, si è ritenuto opportuno effettuare alcune note e approfondimenti su tale aspetto.

2.2 **Consulenza**.

Lo svolgimento di compiti consultivi in materia di protezione dei dati personali nei confronti delle strutture interne ha costituito fin dall'avvio della sua attività una componente non trascurabile dell'operatività del RPD.

Tale funzione, distinta da quella inerente ai processi tipici disciplinati dagli artt. 33 e 35 del GDPR (valutazione dei *data breach* e valutazioni di impatto) è chiaramente individuata dalle norme e raccomandata dagli orientamenti in materia.

Nell'anno trascorso, la consulenza del RPD è stata richiesta in diversi casi, quali:

- *gli adempimenti connessi alle attività volte a fronteggiare l'epidemia da Covid-19*, per la quale il RPD è stato consultato in merito all'individuazione, alla luce delle norme del GDPR, della base giuridica del trattamento delle informazioni rese dal dipendente e dagli studenti e ai sistemi informatici utilizzati per il trattamento;
- *la revisione di molteplici Accordi di collaborazione scientifica e di ricerca* la consulenza ha avuto l'obiettivo di assicurare il puntuale rispetto della normativa sulla protezione dei dati personali nella stipula dei vari attraverso un confronto diretto con l'Area ricerca, trasferimento tecnologico e Gestione progetti e i singoli docenti responsabili dei progetti in oggetto;

Il ruolo consulenziale del RPD, infine, si è estrinsecato nella continua partecipazione a gruppi di lavoro interni e nel costante confronto con le varie strutture su questioni applicative della disciplina sulla *privacy*. In particolare, è costante l'attività di consulenza sulla prevenzione di potenziali violazioni dei dati personali a fronte di episodi di accesso reiterato da parte di soggetti privati e sulla conformità del trattamento dati effettuato da UNICAM, nell'adempimento dei doveri di datore di lavoro, per la gestione dei casi di contagio da Covid-19, secondo gli orientamenti del Garante *privacy*.

2.3 **Le valutazioni di impatto sulla protezione dei dati (DPIA)**

Nel corso del 2021 il RPD ha anche fornito il suo parere per DPIA [2] riguardanti trattamenti di dati di diversa complessità e ampiezza, in relazione a nuovi progetti e

[2] L'art. 35 del GDPR prevede che: «*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati...* ».

procedure che hanno interessato diverse aree dell'Ateneo.

2.4 Le segnalazioni dei data breach.

L'analisi degli eventi configurabili come *data breach* in ottemperanza al GDPR è fondamento della *accountability* del Titolare del trattamento, che ha il dovere di mettere in atto nella propria organizzazione tutte le misure atte a prevenire il rischio di trattamento non conforme dei dati personali e di responsabilità civile derivante dalla lesione della riservatezza che rechi un danno agli interessati.

Il GDPR (art. 33), infatti, quando si verifica un data breach, impone al Titolare del trattamento dei dati di darne notifica alla competente Autorità Garante, entro 72 ore dal momento in cui ne ha avuto conoscenza (salvo giustificazione dei motivi del ritardo, ove la notifica non possa essere effettuata entro tale stringente termine) e qualora, poi, la violazione presenti un rischio elevato per le libertà e i diritti individuali, di darne comunicazione, senza ingiustificato ritardo, anche agli interessati.

Nel corso del 2021 non sono stati segnalati casi di data breach riconducibili a trattamenti effettuati da UNICAM o dai Responsabili designati dal Titolare.

3. Linee di sviluppo.

Nell'assicurare lo svolgimento di tutti i compiti tipici (monitoraggio del Registro dei trattamenti e *assessment* dei trattamenti, pareri relativi a DPIA e a *data breach*), l'impegno del RPD dovrà proseguire secondo quanto già iniziato nel corso del 2021.

Si renderà verosimilmente necessario allargare l'azione di sorveglianza sulla conformità dei trattamenti di dati, specialmente di quelli che più possono avere riflessi sull'immagine e sulla responsabilità dell'Istituto, mediante un'opportuna selezione in base alla rischiosità intrinseca, dedicando un *focus* particolare ai trattamenti di dati che vengano affidati a terzi nell'ambito delle esternalizzazioni.

Per consolidare l'*accountability* di UNICAM quale Titolare dei trattamenti di dati, in ottemperanza a una specifica previsione del GDPR, occorrerà anche verificare nel tempo l'adeguatezza delle misure di protezione dei dati già messe in atto, in relazione all'evoluzione delle regole e delle procedure che ne implicano il trattamento.

Dovrà essere svolta una rivalutazione dei trattamenti "pregressi", ossia antecedenti all'applicazione del GDPR, che presumibilmente porterà in luce l'esigenza di sottoporne un consistente numero a valutazione di impatto: la collaborazione del RPD sarà in quest'ambito orientata a individuare forme di semplificazione del processo di DPIA, per completare in un ragionevole arco di tempo la verifica di adeguatezza di tutti i trattamenti di dati.

In ordine alla valutazione delle misure tecniche di protezione dei dati, saranno promosse iniziative di semplificazione per individuare, con la collaborazione con l'Area infrastrutture, servizi informatici e amministrazione digitale, le misure di sicurezza da considerare "ricorrenti" in quanto di norma adottate in tutti i servizi informatici offerti, allo scopo di agevolare le strutture nella presentazione delle valutazioni di impatto.

3.1 Sorveglianza. Registro delle attività di trattamento.

L'attività di sorveglianza del RPD nel 2022 dovrà avvenire secondo due direttrici di azione:

***A. Il monitoraggio periodico sul complesso delle informazioni iscritte nel Registro delle attività di trattamento*.**

Il RPD condurrà con cadenza semestrale il monitoraggio del Registro delle attività di trattamento, che costituisce uno dei principali elementi di *accountability* del Titolare dei trattamenti, in quanto fornisce un quadro aggiornato dei trattamenti in essere all'interno dell'organizzazione ed è indispensabile per ogni attività di valutazione o analisi del rischio di violazione dei diritti delle persone. Il monitoraggio ha l'obiettivo di verificare la completezza e la coerenza delle descrizioni dei trattamenti ivi censiti

B. L'analisi approfondita (assessment) dei singoli trattamenti.

L'analisi è condotta di norma nell'ambito di incontri con gli uffici/aree e strutture, nei quali vengono approfondite le caratteristiche dei singoli trattamenti nel contesto delle attività svolte per verificarne la corrispondenza con le informazioni dichiarate nel Registro, anche nell'individuare tempi di conservazione coerenti col principio di minimizzazione. Sul tema della conservazione dei dati influisce la questione del coordinamento normativo tra il principio di limitazione della conservazione e quello di integrità del documento digitale che incorpora i dati: soprattutto per le Pubbliche Amministrazioni sussistono infatti incertezze sul rapporto tra vincoli *privacy* e "massimario di scarto" ancora non risolte dalle autorità di settore (Garante *Privacy* e Autorità Archivistica). Infatti l'art. 5, par. 1, lett. e) del GDPR impone che i dati personali siano conservati «*per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati*»; per contro l'art. 10 del d.lgs. 42/2004 (Codice dei beni culturali) qualifica tutti i documenti della PA come "*beni culturali*" e quindi: i) *«non possono essere distrutti, deteriorati, danneggiati o adibiti ad usi non compatibili con il loro carattere storico o artistico oppure tali da recare pregiudizio alla loro conservazione»* (art. 20); ii) devono essere conservati (per i tempi previsti dai piani di conservazione) e, trascorsi 40 anni, ove ne ricorrano le condizioni (massimario di scarto), inviati all'archivio storico.

Per la valutazione dei diversi elementi caratteristici (natura dei dati trattati, finalità e modalità di raccolta, designazione dei dipendenti autorizzati, base giuridica, esigenze di conservazione, informative agli interessati, ecc.) ci si avvarrà di un questionario elaborato secondo le indicazioni del Manuale europeo del RPD.

Nell'analisi dei singoli trattamenti, nell'eventualità di accordi stipulati dalla Banca con terzi, si dovrà verificare in particolare, in base alle attività affidate, se tali soggetti siano stati correttamente qualificati come Responsabili del trattamento per conto della Banca o Titolari autonomi del trattamento ai fini degli obblighi di protezione dei dati.

Per individuare i trattamenti da sottoporre prioritariamente ad *assessment* si continuerà a seguire il principio di selezione degli interventi in relazione al rischio per gli

interessati, che il regolamento europeo pone alla base dell'azione di sorveglianza del RPD.

4. Riflessioni e raccomandazioni finali.

Il Data Protection Officer (D.P.O.), in Italia RPD, rappresenta una nuova figura istituita dal GDPR, da collocare all'interno dell'organigramma aziendale privacy, che è stata mutuata dal Legislatore comunitario dalla legislazione americana ove tale professionista è già previsto. Il suo compito principale è di vigilare sulla corretta applicazione della normativa in materia di protezione dei dati personali, da parte dell'ente/organizzazione.

Con la costituzione del Gruppo di Supporto, UNICAM ha messo adisposizione del RPD personale che consenta di poter meglio affrontare le problematiche che l'applicazione della normativa comporta, e che persegua anche l'obiettivo di formare una ***cultura del rispetto della riservatezza altrui*** all'interno di UNICAM.

A tal fine, si invita il Titolare, e quanti a vario titolo abbiano ruoli gestionali, a coinvolgere ancor più sistematicamente il proprio RPD anche in relazione ad attività quali accertamenti ispettivi, audizioni, richieste di parere o riunioni svolte a qualsiasi titolo, che impattino sul trattamento dei dati. La presenza di una figura qualificata ed esperta in materia e che conosce nel dettaglio i trattamenti svolti, è in grado di assicurare una più corretta e completa rappresentazione delle questioni trattate e delle eventuali iniziative da suggerire – pur rimanendo il potere decisionale in capo al titolare del trattamento.