CLAVIS
CONSULTANTS LAWYERS
ACCOUNTANTS

Nicola Francione (Privacy Department)
Camillo Campli (DPO)

Privacy Department
n.francione@clavisroma.com
www.clavisroma.com

Questioni sul GDPR (Giugno 2018)

Questions on GDPR (June 2018)

CLAVIS
CONSULTANTS LAWYERS
ACCOUNTANTS

ITA	ENG
Questione n. 1 **Per la corretta applicazione del GDPR è necessario conoscere la normativa nazionale?** Occorre partire da alcuni punti normativi del GDPR (Regolamento UE n° 679/2016): *-Considerando n. 8:* "*Ove il presente regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, gli Stati membri possono, nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano, integrare elementi del presente regolamento nel proprio diritto nazionale.*" ; *-Considerando n. 10:* "*Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. Per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento. In combinato disposto con la legislazione generale e orizzontale in materia di protezione dei dati che attua la direttiva 95/46/CE gli Stati membri dispongono di varie leggi settoriali in settori che richiedono disposizioni più specifiche. Il presente regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali («dati sensibili»). In tal senso, il presente regolamento non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito.*" Sulla base dei Considerando 8 e 10, è possibile esprimere alcune riflessioni in merito all'opportunità/obbligo, da parte di chi applica il GDPR, di conoscere la legge nazionale di riferimento. Il GDPR è un Regolamento comunitario, e come tale si applica direttamente in tutti gli Stati Membri e per tutti gli interessati (artt. 2 e 3 GDPR): il Regolamento abroga la disciplina della precedente Direttiva 95/46, che aveva dato origine al Codice della Privacy italiano ed a molte legislazioni in materia nazionali.	**Question n. 1** **For correctly applying GDPR do we need to know the national legislation?** It is needed to fix some points of the GDPR (EU Regulation No. 679/2016): *- Recital n. 8*: "*Where this Regulation provides for specifications or limitations of its rules by the law of the Member States, Member States may, to the extent necessary for consistency and to make national provisions understandable to the persons they apply to, incorporate elements of this Regulation into the own national law.*"; *- Recital n. 10:* "*In order to ensure a consistent and high level of protection for natural persons and to remove obstacles to the circulation of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. It is appropriate to ensure a consistent and homogeneous application of the rules protecting the fundamental rights and freedoms of natural persons with regard to the processing of personal data throughout the Union. With regard to the processing of personal data for the fulfillment of a legal obligation, for the execution of a task carried out in the public interest or in connection with the exercise of official authority vested in the controller, Member States should remain free to maintain or introduce national rules in order to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal data protection legislation implementing Directive 95/46 / EC, Member States have various sectoral laws in areas requiring more specific provisions. This Regulation also provides for a margin for maneuver by the Member States to specify their rules, including with regard to the treatment of particular categories of personal data ('sensitive data'). In this sense, this regulation does not rule out the right of Member States to lay down the conditions for specific treatment situations, including by determining more precisely the conditions under which the processing of personal data is lawful. "* On the basis of Recital 8 and 10, we can express some considerations on the opportunity/obligation, by those who apply the GDPR, to know the national law of reference. The GDPR is a Community Regulation, and as such it is applied directly in all Member States and for all interested parties (articles 2 and 3 GDPR): the Regulation repeals the provisions of the previous Directive 95/46, which had generated the Italian Privacy Code and many national laws. Although remaining formally in force, it is clear that the provisions of Legislative Decree no. 196/2003 (Italian Privacy Code), have become obsolete with the new regulations. In fact, they must be disapplied today, because they are not be able to find more space in contrast with the GDPR, pending implementation decree that should abrogate expressly the old Italian Privacy Code (which will expire next August 21st)

Pur rimanendo formalmente in vigore, è evidente che le disposizioni del d.lgs. 196/2003 (Codice Privacy italiano), sono divenute obsolete con la nuova disciplina. Di fatto, esse devono essere ad oggi disapplicate, non potendo trovare più spazio ove contrastino con il GDPR, in attesa del decreto attuativo che dovrebbe abrogare espressamente il vecchio Codice Privacy italiano (che scadrà il prossimo 21 agosto) per quanto incompatibile ed aggiornarlo alle condizioni poste dal GDPR. Tuttavia, nonostante il GDPR sia fonte gerarchicamente sovraordinata rispetto alle leggi nazionali, sarebbe comunque opportuno conoscere la normativa particolare del singolo Stato. Tale conoscenza è opportuna per quei settori (prevalentemente connessi alla sfera pubblica o a interessi meritevoli di particolare tutela) in cui gli Stati conservino margini di autonomia. È lo stesso GDPR, di volta in volta, a prevedere all'interno delle sue disposizioni, un certo margine di manovra per le autorità nazionali. Ad esempio, gli Stati Membri potranno conservare un certo spazio di manovra in quanto alla determinazione di diritti costituzionali (es. libertà di espressione, trasparenza delle pubbliche amministrazioni, ecc.) o in settori considerati particolarmente a rischio, per le tipologie di dati trattati (ad esempio, in ambito sanitario). Inoltre, se è vero che il GDPR "travolge" la precedente normativa nazionale sulla Privacy (e quindi non pone particolari problemi in merito alla conoscenza di quello specifico settore della legge nazionale), non si può certo stabilire che abbia lo stesso effetto travolgente in tutti gli altri campi. Ad esempio, la base del trattamento giuridico ai sensi dell'art. 6.1.c. GDPR è l'adempimento di un obbligo legale a cui è soggetto il Titolare del Trattamento (*Data Controller*). Ora, sebbene sia chiaro che il Titolare del Trattamento saprà indicare e conoscerà la base normativa su cui si trova ad operare, è ovvio che una conoscenza diretta, a monte, da parte del consulente o del Responsabile della Protezione dei Dati (RPD o DPO-Data Protection Officer) sia certamente preferibile, senza considerare poi le problematiche connesse ad istituti giuridici sconosciuti al nostro ordinamento e presenti negli altri. In definitiva, quando si opera in ambito privacy, non essendo mai tale disciplina "fine a se stessa", ma dovendola ogni volta contemperare e bilanciare con altri diritti e interessi, è preferibile conoscere la normativa di uno Stato, per una piena consapevolezza e visione sistematica. Tale conoscenza delle disposizioni nazionali, in sostanza, sarà poi maggiormente opportuna a seconda del tipo di dati, di trattamenti, di interessi e finalità in gioco.	as incompatible and update it to the conditions placed by the GDPR. However, despite the GDPR being a hierarchically higher-level source than national laws, it would still be appropriate to know the particular legislation of the individual State. This knowledge is appropriate for those sectors (mainly related to the public area or to interests worthy of special protection) in which the States maintain spaces of autonomy. It is GDPR itself, from time to time, to include within its provisions a certain room for maneuver for national authorities. For example, Member States will retain some room for maneuver as regards the determination of constitutional rights (eg freedom of expression, transparency of public administrations, etc.) or in sectors considered to be particularly at risk, for the types of data processed (for example, in the health area). Moreover, if it is true that the GDPR "overwhelms" the previous national legislation on Privacy (and therefore does not pose particular problems with regard to the knowledge of that specific field of national law), it can not be determined that it has the same overwhelming effect in all other fields. For example, the basis of the legal treatment pursuant to art. 6.1.c. GDPR is the fulfillment of a legal obligation to which the Data Controller is subject. Now, although it is clear that the Data Controller will be able to indicate and know the normative base on which it operates, it is obvious that direct knowledge, upstream, by the consultant or the Data Protection Officer (DPO) is certainly preferable, without considering then the problems related to legal institutions unknown to our system and present in others. Ultimately, when working in the field of privacy, never being such an "end in itself" discipline, but every time having to reconcile and balance with other rights and interests, it is preferable to know the legislation of a State, for full awareness and vision systematic. This knowledge of the national provisions, in essence, will then be more appropriate depending on the type of data, treatments, interests and objectives at stake

CLAVIS
CONSULTANTS LAWYERS ACCOUNTANTS

 *Case Law:* *Quesito: è applicabile il GDPR al Principato di Monaco?* La protezione dei dati nel Principato di Monaco è regolata da: - Legge sulla protezione dei dati n. 1.165 del 23.12.1993 (detta "DPA", modificata di volta in volta: - in particolare, Legge n. 1.353 del 4.12.2008; - Legge n. 1.454 del 30.10.2017. Inoltre: - fa parte del Consiglio d'Europa; - è entrato nella Convenzione n. 108 del Consiglio Europeo; - non fa parte dell'UE: di conseguenza non ha recepito la Direttiva 95/46/CE sulla protezione dei dati. Non possiamo affermare che, poiché il Principato di Monaco è uno Stato non/extra-UE, il GDPR non si applica ai soggetti (persone fisiche o giuridiche) monegasche. Il GDPR è applicabile anche a soggetti/società stabiliti al di fuori dell'UE che trattano dati personali di persone fisiche nell'UE per offrire beni e servizi o per monitorare il comportamento di tali persone nella UE. I principi di base dei due atti legislativi sono simili (Legge sulla protezione dei dati monegasca citata, L. n. 1.165 del 23.011.1993) consolidata dalla citata legge n. 1.454 del 30.11.2017). Tuttavia, il GDPR introduce nuovi e diversi requisiti ed esigenze che potrebbero richiedere, per le organizzazioni monegasche interessate, nuove politiche, processi aziendali e tecnologie. Esistono molte differenze tra il sistema del DPA ed il GDPR[1].	 *Case Law:* *Question: is the GDPR applicable to the Principality of Monaco?* Data protection in the Principality of Monaco:: - is regulated by Data Protection Act n. 1,165 of 23.12.1993 (called "DPA"), amended from time to time, and; - in particular, Law No. 1.353 of 4.12.2008; - Law No. 1.454 of 30.10.2017. Furthermore: - it is part of the Council of Europe; - it has entered into Convention no. 108 of the European Council; - it is not part of the EU: as a result, it has not implemented the Directive 95/46/UE on data protection. We cannot determine that, because the Principality of Monaco is a non/extra-EU state, the GDPR does not apply to Monegasque subjects (natural or legal persons). The GDPR is also applicable to persons/companies established outside the EU who process personal data of peoples in the EU to offer goods and services or to monitor the behavior of such persons in the EU. The basic principles of the two legislative acts are similar (the Monegasque Data Protection Act cited, Law No. 1,165 dated 23/01/1993), consolidated by the aforementioned Law no. 1,454 of 30.11 2017). However, the GDPR introduces new and different requirements and requirements that may require new policies, business processes and technologies for the Monegasque organizations concerned. There are main differences between the DPA and the GDPR[1]

[1] **SCHEMA differenze tra GDPR (UE) e DPA (Monaco)** **SCHEME diferences between GDPR (UE) and DPA (Monaco)**

ITA	GDPR	DPA	ENG	GDPR	DPA
Persone protette	protegge esclusivamente i dati personali di persone fisiche	protegge quelli di persone sia fisiche che giuridiche	*Protected people*	protects the personal data of natural persons	protects those of both physical and legal persons.
Applicazione extraterritoriale	contiene una regola di applicazione extraterritoriale, al fine di evitare l'elusione della legislazione europea da parte di un responsabile del trattamento o di un subcontraente la cui sede non si trova sul territorio UE, ma che tratta i dati personali relativa alle persone fisiche che risiedono sul territorio dell'UE. , le attività di trattamento devono essere collegate alla fornitura di beni o servizi (indipendentemente dal fatto che sia richiesto o meno un pagamento) alle persone interessate nella UE o all'osservazione del comportamento umano intervenendo nella UE	Non esiste	*Extraterritorial application*	contains an extraterritorial application rule that does not exist under the Monegasque DPA, in order to avoid the circumvention of European legislation by a controller or subcontractor whose headquarters are not located on EU territory, but which deals with personal data relating to natural persons residing in the territory of the EU. In order for the GDPR to be applicable to such data controllers or subcontractors, processing activities must be linked to the supply of goods or services (regardless of whether or not a payment is required) to the persons concerned in the EU or to the observation of human behavior by intervening in the EU.	not expected
Consenso dell'interessato	presta particolare attenzione al consenso dell'interessato (definizione, condizioni applicabili al consenso),	minore attenzione Il consenso a condizioni generali contenenti un'accettazione del trattamento dei dati potrebbe essere insufficiente per il GDPR.	*Consent of the interested person*	particular attention to the consent of the interested party (definition, conditions applicable to consent), with respect to the Monegasque DPA. In particular, in the context of a written consent statement, which also covers other issues, the request for consent must be in a form that clearly distinguishes it from other statements in a way that is understandable and easily accessible.	This rule should entail a new independent consideration of the "contract" and "privacy" consents. The consent to general conditions containing an acceptance of data processing may therefore be insufficient in the light of the GDPR
Diritti dell'interessato: tipologia dei diritti	prevede un obbligo di informazione rafforzato per le persone interessate dal trattamento dei dati	non lo prevede	*Rights of the interested party* *See below types*	provides for a reinforced information obligation for data subjects	not expected

1) informazione	prevede ad esempio: la base giuridica del trattamento, gli interessi legittimi, la volontà di trasferire dati verso un paese terzo, l'assenza di una decisione di adeguatezza del livello di protezione, l'esistenza di processi decisionali automatizzati (profilazione), il periodo di conservazione dei dati.	non lo prevede	*1) information*	provides for example: the legal basis of the processing, legitimate interests, the willingness to transfer data to a third country, the absence of a decision of adequacy of the level of protection, the existence of automated decision-making processes (profiling), the period data retention.	not expected
2) accesso	innova per quanto riguarda le informazioni specifiche da fornire in seguito all'esercizio del diritto di accesso, prevedendo espressamente: il periodo di conservazione, il diritto di rettifica e cancellazione, il diritto di presentare reclamo all'Autorità di Vigilanza, le garanzie particolari adottate per i trasferimenti di dati verso un paese terzo.	non lo prevede	*2) access*	as regards the specific information to be provided following the exercise of the right of access, expressly providing for: the retention period, the right of rectification and cancellation, the right to complain to the Supervisory Authority, the special guarantees adopted for transfers of data to a third country.	not expected
3) oblio	è più chiaro e stabilisce le condizioni per l'esercizio del diritto all'oblio digitale. , il Responsabile del Trattamento dei dati che ha reso pubblici i dati ha l'obbligo di informare le altre persone responsabili del trattamento, della richiesta dell'interessato di cancellare qualsiasi collegamento a dati, copie o riproduzioni.	lo previsto	*3) to be cancelled*	it is clearer and establishes the conditions for the exercise of the right to digital forgetting. , the Data Processor who made the data public has the obligation to inform the other persons responsible for the processing of the data subject's request to cancel any connection to data, copies or reproductions.	expected
4) limitazione	prevede il diritto di etichettare i dati personali registrati, al fine di limitare il loro futuro trattamento, che autorizza in casi elencati	Non lo prevede	*4) limitation*	provides the right to label personal data recorded, in order to limit their future processing, which authorizes in listed cases	not expected
5) opposizione	circoscrive il diritto di opposizione per motivi relativi alla particolare situazione della persona interessata a due sole ipotesi di trattamento e il responsabile del trattamento può rifiutare condizionalmente di applicare il diritto di opposizione	stabilisce il principio dell'esercizio del diritto di opposizione per motivi legittimi e prevede eccezioni	*5) opposition*	circumscribes the right of opposition on grounds relating to the particular situation of the person concerned to only two cases of treatment and the controller can refuse to apply the right to objectively.	establishes the principle of exercising the right of opposition for legitimate reasons and provides for exceptions
6) portabilità	lo prevede	non lo prevede	*6) portability*	Expected	not expected

Titolare del trattamento	lo prevede - onere di dimostrare la conformità delle attività di trattamento e l'efficacia delle misure tecniche e organizzative adottate per garantire un livello di sicurezza adeguato al rischio, che descrive in dettaglio. In luogo dell'obbligo del controllore della notifica preventiva all'Autorità di vigilanza, il GDPR impone l'obbligo di tenere un registro documentale delle operazioni di trattamento, con un'eccezione per le società o organizzazioni con meno di 250 dipendenti (a meno che il trattamento sia regolare o è probabile che crei un rischio elevato per i diritti e le libertà). Gli obblighi derivano dai principi di protezione dei dati dalla progettazione del trattamento (protezione dei dati in base alla progettazione - *privacy by design*) e dalle impostazioni predefinite (protezione dei dati per impostazione predefinita – *privacy by default*), per garantire che le misure di protezione dei dati siano integrate nei prodotti e servizi sin dalle prime fasi di sviluppo. Ha l'obbligo di informare l'autorità di vigilanza di eventuali violazioni dei dati personali e di comunicare all'interessato qualsiasi violazione che possa creare un rischio elevato per i diritti e le libertà. Deve eseguire una valutazione dell'impatto prima del trattamento. Deve nominare un Responsabile della Protezione dei dati (DPO)	non lo prevede	*Data Controller*	he predicts it - the burden of demonstrating the compliance of processing activities and the effectiveness of technical and organizational measures taken to ensure a level of safety appropriate to the risk, which is described in detail. In place of the obligation of the controller for prior notification to the Supervisory Authority, the GDPR imposes the obligation to keep a record of the processing operations, with an exception for companies or organizations with less than 250 employees (unless treatment is regular or likely to create a high risk for rights and freedoms). The obligations derive from the principles of data protection from the design of the treatment (data protection by design - privacy by design) and the default settings (data protection by default - privacy by default), to ensure that protection measures data are integrated into products and services from the early stages of development. It is obliged to inform the supervisory authority of any violation of personal data and to inform the data subject of any violation that could create a high risk for rights and freedoms. It must perform an impact assessment before treatment. Must appoint a Data Protection Officer (DPO)	not expected
Controllore Congiunto	lo prevede con regime giuridico specifico	lo prevede, ma non prevede un regime giuridico specifico	*Joint Controller*	Expected with a specific legal regime	Expected without a specific legal regime
Subcontraenti	amplifica gli obblighi dei subcontraenti e organizza un regime di subcontratto, che è separato dalle funzioni di sicurezza. Previsto anche l'obbligo del subcontraente estero quando il GDPR applica alle sue attività, di nominare un Rappresentante con sede nell'UE, con alcune eccezioni	non è previsto un regime specifico: solo nomina di un Rappresentante del controllore stabilito all'estero	*Sucontractors*	amplifies the obligations of subcontractors and organizes a subcontracting regime, which is separate from the security functions. The overseas subcontractor is also required when the GDPR applies to its activities, to appoint a representative based in the EU, with some exceptions	Expected without a specific legal regime: only appointment of a representative of the auditor established abroad

Il GDPR è molto presente a Monaco: le società monegasche che rientrano nel GDPR dovranno adattarsi ad un'altra filosofia di protezione dei dati rispetto a quella del DPA monegasco ad essere sostituita.

Quesito n. 2
Quando è obbligatorio nominare il DPO?
Chi può essere nominato?

Il GDPR, all'art. 37, contempla la nuova figura del "Responsabile Protezione Dati" (RPD o DPO- Data Protection Officer).
La nomina di tale soggetto è prevista come obbligatoria in tre casi:

a) *il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;*
b) *le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure*
c) *le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10".*

Inoltre, è previsto che "*Nei casi diversi da quelli di cui al paragrafo 1, il titolare del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati*".
In pratica, il DPO può essere nominato dal Titolare (*Data Controller*) e/o dal Responsabile del Trattamento (*Data Processor)*, a seconda di chi, in concreto, si trovi nelle fattispecie sopra delineate ed abbia la necessità di

The GDPR is well known in Monaco: the Monegasque companies that fall within the GDPR will have to adapt to another philosophy of data protection compared to that of the Monegasque DPA, destined to be changed.

Question n. 2
When is it needed to name the DPO?
Who can be named?

The GDPR, in art. 37, contemplates the new figure of the "Data Protection Officer" (DPO).
The appointment of this officer is foreseen as needed in three cases:

a) *processing is carried out by a public authority or a public body, with the exception of the courts when they exercise their judicial functions;*
b) the main activities of the data controller or data controller are treatments that, by their nature, scope and/or purpose, require regular and systematic monitoring of data subjects on a large scale; or
c) the main activities of the controller or processor are the large-scale processing of specific categories of personal data referred to in Article 9 or of data relating to criminal convictions and offenses referred to in Article 10 " .

Furthermore, it is provided that "*In other cases than those referred to in paragraph 1, the data controller, the data processor or the associations and other bodies representing the categories of data controllers or data processors may or, if by EU or Member State law, must designate a data protection officer* ".
In practice, the DPO can be appointed by the Data Controller and/or by the Data Processor, depending on who, in practice, is in the cases outlined above and needs the appointment. If both the Data Controller and the Data Processor are need to appoint a DPO, it can be:
- appointed the same subject for both;
- or two distinct DPOs, which will have the duty of mutual collaboration.

In the company groups the DPO can be unique, provided it can effectively carry out its tasks for all the members of the

Trasferimento di dati personali verso paesi terzi	istituisce un "diritto di seguito". I trasferimenti di dati al di fuori della UE sono sottoposti al GDPR per i trasferimenti e per ulteriori elaborazioni e trasferimenti verso un paese terzo. In assenza di una decisione della Commissione Europea che individua un livello adeguato di protezione e nel contesto di un gruppo di società che si trovano a trasferire dati all'interno del gruppo al di fuori della UE, il GDPR incorpora il sistema delle regole vincolanti tra imprese. Il contenuto obbligatorio imposto è molto ampio (principi essenziali, diritti esecutivi), il che implica una revisione per Monaco delle *Binding Corporate Rules* già adottate	non previsto	*Joint Controller*	establishes a "resale right". Transfers of data outside the EU are subject to the GDPR for transfers and for further processing and transfers to a third country. In the absence of a European Commission decision identifying an adequate level of protection and in the context of a group of companies that are transferring data within the group outside the EU, the GDPR incorporates the system of binding rules between companies . The obligatory content imposed is very broad (essential principles, executive rights), which implies a revision for Monaco of the Binding Corporate Rules already adopted	not expected

nomina. Se sia il Titolare del trattamento che il Responsabile si trovano nella necessità di nominare un DPO, può essere:
- nominato il medesimo soggetto per tutti e due;
- oppure due distinti DPO, che avranno dovere di collaborazione reciproca.

Nei gruppi di imprese il DPO può essere unico, a condizione che possa effettivamente svolgere i suoi compiti per tutte le componenti del gruppo.

Il DPO può essere:
- un dipendente del Titolare del Trattamento;
- un dipendente del Responsabile del Trattamento;
- un terzo, che assolve i suoi compiti in base a un contratto di servizi.

Sul punto, è importante chiarire alcuni aspetti:

- la figura del DPO, per come è costruita nel GDPR, costituisce una sorta di raccordo tra autorità Garante Privacy e soggetto che opera il trattamento, quando il Garante richieda chiarimenti sui comportamenti;
- egli deve poter svolgere i propri compiti (individuati all'art. 39 GDPR) nella piena indipendenza e senza ricevere alcun tipo di istruzione/direttiva, e riferirà e comunicherà direttamente al vertice del soggetto che lo ha designato. Ciò significa che, qualora si designi un DPO interno, è opportuno che lo stesso sia un soggetto che possa relazionarsi con il Titolare "alla pari". Questo per evitare che il DPO, la cui funzione è quella di far rispettare il GDPR e di interfacciarsi con il Garante ed eventuali Interessati, si trovi in situazioni "scomode" che non gli consentano di assolvere appieno i propri compiti. Un DPO non può sottostare al timore di subire ripercussioni dal Titolare qualora debba dar conto di violazioni del GDPR. Ad esempio: il DPO dice al titolare di adempiere ai compiti A, B, e C, ed il Titolare adempie ad A e B, ma tralascia C (incorrendo quindi nel rischio di subire sanzioni);
- il DPO, per provare di aver svolto correttamente il proprio compito e non incorrere a sua volta in responsabilità (non ha fornito le indicazioni necessarie al Titolare) e reati (false dichiarazioni), dovrà annotare tale inadempienza del Titolare: è chiaro che, se subisse anche solo l'astratta minaccia di licenziamenti/demansionamenti, si troverebbe in una posizione in cui non potrebbe farlo con la dovuta serenità ed indipendenza, e quindi, di fatto, sarebbe qualificato come una "testa di legno", una figura "fantoccio";
- se così fosse, è importante far presente che chiunque sia obbligato alla designazione e nomini un DPO "fantoccio", che operi al servizio e sotto le direttive del Titolare, incorre nella violazione del principio alla base del Regolamento, ossia quello dell'*accountability*: per la violazione di tale principio sono previste sanzioni fino al 4% del fatturato annuo o fino a 20 milioni di euro.

group.

The DPO can be:
- an employee of the Data Controller;
- an employee of the Data Processor;
- a third party, who performs his duties on the basis of a service contract.

On this point, it is important to clarify some aspects:
- the DPO, as it is built in the GDPR, constitutes a sort of connection between the privacy Authority and the subject that operates the treatment, when the Autority requests clarification on behavior;
- he must be able to carry out his duties (identified in Article 39 of the GDPR) in complete independence and without receiving any kind of instruction/directive, and will report and communicate directly to the summit of the person who designated him. This means that, if you designate an internal DPO, it is appropriate that the same is a subject that can relate to the holder "au pair". This is to avoid that the DPO, whose function is to enforce the GDPR and to interface with the Authority and any Interested, is in "uncomfortable" situations that do not allow him to fully fulfill his duties. A DPO can not be subjected to the fear of being affected by the Data Controller if it has to report violations of the GDPR. For example: the DPO tells the holder to perform tasks A, B, and C, and the Data Controller fulfills A and B, but leaves C (thus incurring the risk of being penalized);
- the DPO, to prove that he has done his job correctly and not incur in liability (did not provide the necessary information to the Owner) and offenses (false statements), must note this default of the data Controller: it is clear that, if it suffered even the abstract threat of redundancies/demotions, it would be in a position where it could not do it with due serenity and independence, and therefore, in fact, would be qualified as a "wooden head", a "puppet" figure;
- if so, it is important to point out that whoever is obliged to designate and appoint a "puppet" DPO, who operates in the service and under the directives of the Owner, violates the principle underlying the Regulation, namely that of accountability: for violation of this principle, penalties of up to 4% of annual turnover or up to 20 million euros are provided for.
- Therefore, it is not appropriate to appoint an internal DPO that cannot effectively perform its duties with due independence;
- The Italian Privacy Authority then clarified that, with regard to the absence of a conflict of interest, it is not recommended (for individuals) to appoint top managers, who can determine the means and methods of data processing;
- with regard to the Public Administrations, still obliged to appoint the DPO, the same Authority, in December 2017, clarified that the appointed person could be a high-level manager or official. Nominating an internal DPO means identifying a top subject who, however, has no decision-making role regarding treatments, or an actual subordinate who is provided with the assistance and the means necessary to fulfill his/her role.

- Pertanto, non è opportuno nominare un DPO interno che non possa effettivamente svolgere le proprie mansioni con la dovuta indipendenza; - Il Garante Privacy italiano ha chiarito poi che, per quel che riguarda l'assenza del conflitto di interessi, si sconsiglia (per i privati) la nomina di soggetti apicali, che possano determinare mezzi e modalità del trattamento dei dati; - quanto alle Pubbliche Amministrazioni, sempre obbligate alla nomina del DPO, lo stesso Garante, nel dicembre 2017, ha chiarito che il soggetto nominato possa essere un dirigente o funzionario di alta qualifica. Nominare un DPO interno significa individuare un soggetto apicale che però non abbia alcun ruolo decisionale in merito ai trattamenti, o un effettivo subordinato che sia fornito dell'assistenza e dei mezzi necessari per adempiere al proprio ruolo.	
<u>Questione n° 3</u> **Quali caratteristiche deve avere il DPO?** **Quali responsabilità ha?** Per ciò che concerne la responsabilità del DPO, va specificato che egli deve (o dovrebbe) essere un professionista altamente qualificato, con competenze e <u>conoscenze specifiche ed in costante aggiornamento</u> sulla normativa privacy, in ambito informatico e di sicurezza. La *compliance* al GDPR richiede un approccio trasversale dove le materie sopra elencate si intrecciano. È quindi estremamente difficile che un DPO abbia tutte le alte e specifiche capacità richieste. Per questo motivo, è opportuno che lo stesso si avvalga di un *team* di esperti/consulenti che lo aiutino nello svolgimento dei compiti. Fatta tale premessa, la qualificazione del DPO come figura altamente professionale rende difficile immaginare che un tale soggetto sia esente da responsabilità. Sul punto, l'art. 39 del Regolamento individua il <u>contenuto minimo</u> dei compiti del DPO: ciò significa che un atto di designazione o contratto con cui si nomini un DPO (interno o esterno) dovrà contenere tutte le indicazioni ex art. 39, più altri eventuali obblighi per il DPO. Il mancato rispetto di tali obblighi, qualora siano comminate sanzioni al Titolare del Trattamento per violazioni del GDPR, implica <u>responsabilità contrattuale</u> del DPO. Più nel dettaglio, spetta al Titolare del Trattamento o al Responsabile del Trattamento garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR. La responsabilità di garantire l'osservanza della normativa in materia di protezione dei dati ricade sul Titolare del Trattamento o sul Responsabile del Trattamento. Le sanzioni che potranno essere comminate ex artt. 83 e 84 saranno a carico di Titolare/Responsabile del Trattamento.	**<u>Question n° 3</u>** **What features must the DPO have?** **What liabilities does he have?** Regarding to the liability of the DPO, it should be specified that he must (or should) be a highly qualified professional, with specific skills and knowledge and constantly updated on privacy legislation, in information technology and security. Compliance with the GDPR requires a cross-cutting approach where the subjects listed above are interconnected. It is therefore extremely difficult for a DPO to have all the high and specific skills required. For this reason, it is appropriate that the same make use of a team of experts/consultants who help him in carrying out the tasks. With this premise, the qualification of the DPO as a highly professional figure makes it difficult to imagine that such a subject is exempt from liability. On the point, the art. 39 of the Regulation identifies the minimum content of the DPO's duties: this means that an act of designation or contract with which a DPO is nominated (internal or external) must contain all the indications pursuant to art. 39, plus other possible obligations for the DPO. Failure to comply with these obligations, if sanctions are imposed on the Data Controller for breaches of the GDPR, implies contractual liability of the DPO. More in detail, it is up to the Data Controller or the Data Processor to guarantee and be able to demonstrate that the processing is carried out in accordance with the GDPR. The liability for ensuring compliance with data protection regulations lies on Data Controller or Data Processor. The penalties that may be imposed pursuant to art. 83 and 84 will be borne by the Data Controller or Data Processor. However, if they have acted on the indications of the DPO (which has misdirected, poorly supervised, etc.), they may act in recourse against him, according to the canons of liability ex art. 1218 and 2236 (Italian) Civile Code. So even in the event that some people request compensation for

Tuttavia, qualora questi abbiano agito su indicazioni del DPO (che abbia mal consigliato, mal sorvegliato, ecc.) potranno agire in regresso contro lo stesso, secondo i canoni della responsabilità ex artt. 1218 e 2236 c.c. Così anche nel caso in cui qualche interessato richieda un risarcimento danni, lo chiederà al Titolare o al Responsabile, che poi si rivarranno eventualmente sul DPO inadempiente, sempre *ex contratto*. Chiunque dichiari di aver subito un danno in seguito a violazione dell'art. 82 del GDPR, deve fornire indicazioni di tale violazione; il Titolare/Responsabile potranno rispondere ex art. 2043 c.c., nei confronti dei terzi, salvo dimostrino che il fatto non sia a loro in alcun modo imputabile (e qui si torna ad un eventuale regresso verso il DPO inadempiente). Azione diretta degli interessati contro il DPO è più difficile immaginarla: plausibilmente sarà ex art. 2043 c.c., nei casi in cui gli stessi dimostrino il dolo o la colpa grave del DPO nei confronti dei terzi.	damages, they will ask the Owner or the Manager, who then will eventually be on the defaulting DPO, always ex contract. Anyone who claims to have suffered damage as a result of violation of Article 82 of the GDPR, must provide indications of this violation; the Owner/Manager will be liable under article 2043 (Italian) Civile Code, towards third party, unless they prove that the fact is not in any way imputable (and here we return to a possible regression to the defaulting DPO). Direct action by data subjects against the DPO is more difficult to imagine: plausibly it will be under article 2043 (Italian) Civile Code, in cases where the same prove the fraud or gross negligence of the DPO.
Questione n° 4 **In Italia: il GDPR è applicabile già dal 25 maggio 2018 oppure occorre attendere il decreto attuativo (del 22 agosto 2018)?** In Italia, il GDPR non è stato prorogato: esso è pienamente applicabile, quindi valido ed efficace, fin dal 25 maggio 2018, indipendentemente dall'entrata in vigore del decreto attuativo italiano (per cui la delega al Governo è esercitabile entro il 22 agosto 2018, avendo mancato la scadenza del 21 maggio). Per effetto della divenuta applicabilità, nonostante le voci e le incertezze che circolano in questi giorni, possiamo porre alcuni punti fissi, qui riassunti: - in mancanza del decreto di adeguamento italiano, la soluzione compatibile con l'ordinamento italiano ed europeo è che l'intero Codice Privacy, per la parte in contrasto col GDPR, non può più essere applicato dopo il 25 maggio 2018; - in questo periodo, fino alla entrata in vigore del decreto di attuazione del GDPR (21.08.2018), si verifica una sovrapposizione tra le disposizioni europee (GDPR) e il Codice Privacy italiano (d.lgs n. 196/ 2003); - il decreto attuativo riguarda alcuni "adattamenti" della normativa italiana al GDPR, andando a riempire gli spazi e i dettagli specifici non coperti dal GDPR; - il decreto attuativo non potrà portare norme in contrasto con il GDPR; - tra le norme del GDPR che non hanno problemi di attuazione, rientrano certamente quelle in tema di data breach e quelle sul DPO (Data Protection Officer); - è del tutto irrilevante, ai fini di accertamento della *compliance* (adeguamento) al GDPR, la pubblicazione del decreto di adeguamento che avverrà dopo il 21.08.2018; - per tali ragioni, i controlli da parte degli organi competenti (Guardia di Finanza) potrebbero scattare già dopo il 25 maggio 2018, come peraltro espressamente dichiarato dai comandanti del Nucleo Speciale Privacy	**Question n° 4** **In Italy: is the GDPR already applicable from 25th of May 2018 or should we wait for the implementing decree (22nd of August 2018)?** In Italy, the GDPR has not been extended: it is fully applicable, therefore valid and effective, as of 25th of May 2018, independently of the entry in force of the Italian implementing Decree (for which the delegation to the Government is exercisable by 22nd of August 2018, having missed the deadline of May the 21st). Due to the effect of the applicability, despite the rumors and the uncertainties circulating these days, we can put some fixed points, summarized here: - in the absence of the Italian implementing Decree, the solution compatible with Italian and European law is that the entire Italian Privacy Code, for the part in contrast with the GDPR, can no longer be applied after May the 25th, 2018; - in this period, up to the entry into force of the Decree implementing the GDPR (21.08.2018), there is an overlap between the European provisions (GDPR) and the Italian Privacy Code (Legislative Decree No. 196/2003); - the implementing decree concerns some "adaptations" of the Italian legislation to the GDPR, filling in the spaces and specific details not covered by the GDPR; - the implementing decree can not bring norms contrary to the GDPR; - among the rules of the GDPR that do not have problems of implementation, are certainly those on the subject of data breach and those on the DPO (Data Protection Officer); - it is totally irrelevant, for the purposes of ascertaining the compliance (adjustment) to the GDPR, the publication of the adjustment decree that will take place after 21.08.2018; - for these reasons, the controls by the competent bodies (GdF-Guardia di Finanza) could take place after May the 25th, 2018, as expressly stated by the commanders of the Special Privacy Unit of the same GdF during the c.d. D-day (25.05.2018);

della stessa GdF nel corso del c.d. D-day (25.05.2018); - è stato infatti dichiarato che le ispezioni partiranno sugli adempimenti obbligatori e fondamentali per l'adeguamento al GDRP: a) nomina del DPO; b) controlli sulle misure previste in caso di *data breach* (non solo in situazioni estreme ma anche in caso di perdita accidentale e occasionale di dati, ad esempio, per furto di un pc, di un *hardisk* ecc.); c) registro dei trattamenti: rappresenta il punto di partenza della attività ispettiva per valutare le misure per la tutela della privacy messe in atto. Alla luce di queste considerazioni, poiché il GDPR è già pienamente in vigore, è necessario procedere da subito all'adeguamento a tale normativa europea (GDPR), senza attendere l'emanazione del decreto attuativo italiano. Questo, peraltro, avrebbe valore esclusivamente per trattamenti di dati italiani. **CLAvis si affianca alle imprese e persone in tutte le fasi di *compliance,* di consulenza e di difesa in materia di Privacy in Italia (Codice della Privacy), in Europa (GDPR) ed a livello internazionale (adeguamento al GDPR dei paesi extra-UE).**	- it was in fact declared that the inspections will start on the obligatory and fundamental obligations for the adjustment to the GDRP: a) appointment of the DPO; b) checks on the measures envisaged in case of data breach (not only in extreme situations but also in case of accidental and occasional loss of data, for example, for theft of a PC, a hardisk etc.); c) treatment register: represents the starting point of the inspection activity to evaluate the measures for the protection of privacy implemented. In light of these considerations, since the GDPR is already fully in force, it is necessary to proceed immediately to the adaptation to this European legislation (GDPR), without waiting for the enactment of the Italian implementing decree. This, moreover, would have value only for Italian data processing. **CLAvis advices companies and people in all phases of compliance, counseling and defending in Privacy area in Italy (Code of Privacy), in Europe (GDPR) and at international level (adaptation to GDPR of non-EU countries).**