CONSIGLIO NAZIONALE
DEGLI INGEGNERI

Legislazione Tecnica
Area Consulenza

ADEMPIMENTI PRIVACY PER ORDINI PROFESSIONLI: PERIMETRO LEGISLATIVO E PRIMISSIME INDICAZIONI OPERATIVE

Incontro formativo

Roma, 17 maggio 2018

Relatore: Rosalisa Lancia

Agenda

- Il contesto di riferimento
- I concetti chiave del GDPR e il nuovo approccio del Legislatore
- il *risk based approach* e l'*accountability*
- *Privacy by design* e *privacy by default*
- Le nuove figure: il *DPO-Data Privacy Officer*
- Privacy e Ordini professionali
- Suggerimenti operativi per Ordini: cosa fare entro il 25 maggio p.v.

Regolamento Generale sulla protezione dei dati - GDPR: Applicazione

- Il 25 maggio 2018 scade il termine per l'adeguamento dei soggetti obbligati al Reg. UE 2016/679 del 27 aprile 2016, rubricato «*Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati*)»
- Il Regolamento, anche detto GDPR – General Data Protection Regulation, adottato 20 anni dopo la Direttiva 95/45/CE da cui è derivato il D.Lgs. 196/20003 (Codice Privacy), è diretto a fornire un quadro più robusto e coerente di tutela dei dati personali e ad assicurare l'omogeneità di regolamentazione nei paesi membri, onde evitare la frammentazione della normativa privacy da stato a stato
- La scelta dello strumento del «Regolamento» (e non di un'altra «direttiva») va esattamente in questa direzione: il Regolamento per essere efficace non necessita -salvo espressa previsione- di un atto legislativo o regolamentare interno del singolo stato membro
- Il GDPR è pertanto ***entrato in vigore, applicabile ed azionabile in Italia sia dal 25 maggio 2016*** e ***il 25 maggio 2018 costituisce il termine ultimo per il suo adeguamento***: il Legislatore comunitario ha previsto una «finestra» di 2 anni per adeguarsi

Il GDPR in Italia

- Con L. 163 del 25 ottobre 2017, il Parlamento italiano relativamente alla nuova privacy, ha previsto che il Governo, entro 6 mesi dall'entrata in vigore della legge stessa e previo parere del Garante Privacy, adotti uno o più decreti legislativi «*al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento*».
- L'emanazione di tale decreto legislativo comporta:
  - ✓ Abrogazione espressa delle disposizioni del Codice Privacy (D.Lgs. 196/2003) incompatibili con il GDPR
  - ✓ Le modifiche del Codice Privacy limitatamente a quanto necessario per dare attuazione alle disposizioni contenute del GDPR
  - ✓ Il coordinamento delle disposizioni del Codice Privacy con quelle del Regolamento
  - ✓ La previsione di specifici provvedimenti attuativi ed integrativi del Garante Privacy ai sensi del GDPR
  - ✓ Adeguamento del sistema sanzionatorio –civile e penale- a quanto previsto del Regolamento

- Alla data 5 maggio 2018 è stata emanata una seconda bozza di «*Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Reg. UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione dei dati personali, nonché alla libera circolazione di tali datai e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)*»
- **La mancata adozione di atti legislativi interni non comporta una posticipazione della scadenza del 25 maggio p.v: il Regolamento è già vigente e vincolante**

Ambito di applicazione del Regolamento

L'applicazione del Regolamento non è collegata all'individuazione di categorie di soggetti obbligati, ma il GDPR si applica ogni qual volta vengano trattati dati personali da parte di qualsiasi soggetto (pubblico o privato, a prescindere dalla dimensione, dall'attività svolta, dal settore in cui opera). Nello specifico:

- Il Regolamento si applica agli «Interessati», ovvero alle persone fisiche, e non anche alle persone giuridiche
- Il Regolamento protegge i diritti e le libertà fondamentali degli Interessati, primi fra tutti il diritto alla protezione dei dati personali, indipendentemente dalla loro nazionalità o residenza
- Il Regolamento si applica al trattamento dei dati personali svolti attraverso strumenti automatizzati e non

Esclusione dell'applicazione

Il Regolamento non si applica in casi tassativi e normativamente individuati, ovvero quando il trattamento:

1. Non ricade nell'ambito dell'applicazione del diritto della UE
2. È svolto dallo Stato membro a fronte di disposizioni specifiche sulla politica estera e di sicurezza comune, come previsto dal trattato sull'Unione Europea (trattato di Lisbona 13 dicembre 2007)
3. È effettuato per finalità personali o domestiche, quindi non a scopi commerciali o professionali
4. È svolto da pubbliche autorità per finalità di sicurezza pubblica e prevenzione dei reati

Direttrici del Regolamento

Il Legislatore comunitario ha predisposto il Regolamento partendo da talune necessità che, successivamente alla Direttiva madre e nel coro di 20 anni si sono manifestate, anche a seguito dell'utilizzo di differenti modalità di comunicazione, nuove tipologie di reati, utilizzo massivo di social network e reti informatiche, nuove esigenze e nuove pratiche che hanno richiesto una razionalizzazione a livello legislativo.

I principali ambiti considerati dal Legislatore UE per la predisposizione del Regolamento sono:

- Cybersecurity e obblighi di comunicazione del c.d. «data breach»
- nomina del Data Privacy Officer
- Consensi
- Trasferimento transfrontaliero dei dati
- Profilazione
- Portabilità dei dati
- Gestione del fornitore
- Pseudonimizzazione
- Codice di condotta e certificazioni
- Sanzioni

Le novità del Regolamento: sintesi

- Nomina del Data Protection Officer ("DPO")
- Tenuta di un «registro delle attività di trattamento»
- Svolgimento di una «valutazione di impatto sulla protezione dei dati»
- Riconoscimento del c.d. «diritto all'oblio», quale possibilità per l'interessato di decidere che siano cancellati e non sottoposti ulteriormente a trattamento i propri dati personali non più necessari per le finalità per le quali sono stati raccolti
- Riconoscimento della «portabilità dei dati», ovvero il diritto dell'interessato di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i suoi dati personali forniti a un titolare del trattamento e il diritto di trasmettere tali dati ad altro titolare del trattamento senza impedimenti, qualora l'interessato abbia fornito il proprio consenso al trattamento o se questo sia necessario per l'esecuzione di un contratto
- Rispetto del principio di «accountability», quale dimostrazione dell'adozione di policy e misure adeguate in conformità al Regolamento
- Rispetto del principio della «privacy by design» (l'attuazione di adeguate misure tecniche e organizzative sia all'atto della progettazione che dell'esecuzione del trattamento) e della «privacy by default» (principio secondo cui i dati vengano trattati solamente per le finalità previste e per il periodo strettamente necessario a tali fini)
- Misure di sicurezza «tailorizzate»
- Inasprimento delle sanzioni
- Procedura per la gestione del «data breach»

Il GDPR – Concetti chiave e nuovo approccio

- L'impianto legislativo del trattamento dei dati derivanti dal GDPR è in continuità con quanto già disposto dalla Direttiva Madre e, quindi, al Codice Privacy – D.Lgs. 2196/2003
- La vera innovazione del GDPR è costituita dall'approccio usato dal Legislatore comunitario, sintetizzabile in due principi:
  - ✓ Principio dell'accountability
  - ✓ Principio del *risk based approach*
- Il combinato disposto dei due principi si traduce in un **generale obbligo, per il Titolare del trattamento e per il Responsabile del trattamento di adottare e porre in esecuzione misure di sicurezza appropriate e coerenti con la natura/entità del trattamento e che siano in grado di «dimostrare» che tali misure implementate assicurino il rispetto del GDPR nello svolgimento del trattamento**

ACCOUNTABILITIY – La responsabilità «verificabile»

Il principio di accountability (responsabilità/rendicontazione) richiede che il titolare del trattamento deve essere **sempre in grado di dimostrare** di **aver rispettato ed essersi conformato alle disposizioni del GDPR**.

RISK BASED APPROACH –RBA

Il RBA richiede che i soggetti destinatari di obblighi sono tenuti ad identificare, valutare e comprendere il rischio sottesto e ad adottare misure di prevenzione commisurate alla tipologia di rischio al fine di gestirlo e mitigarlo con efficienza.

Il GDPR – concetti chiave e nuovo approccio (segue)

- Ai Titolari ed ai Responsabili, si richiede un approccio proattivo e non più reattivo, mediante attività e comportamenti che prevengano in modo effettivo ed efficace il possibile evento di danno, avuto riguardo alle specificità dei diversi trattamenti cui si riferiscono

- Quanto sopra era già oggetto di riflessioni pre-regolamento (*Opinion 3/2010 on the principle of accountability, WP art.29*) in cui – tra l'altro- si raccomandava che il titolare del trattamento dei dati dovesse essere in grado di dimostrare di avere adottato un ***processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali***, anche attraverso ***l'elaborazione di specifici modelli organizzativi*** e che ***dovesse dimostrare in modo positivo e proattivo che i trattamenti di dati effettuati sono adeguati e conformi al regolamento europeo in materia di privacy:***

  ([…] a data controller should […] have in place a privacy management programme […] be prepared to demonstrate its privacy management programme as appropriate […])

- queste considerazioni convergono nell'art. 24 del Regolamento 2016/679 ("*Responsabilità del trattamento*") secondo cui il **Titolare del trattamento** metta in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al presente regolamento, 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 GDPR – concetti chiave e nuovo approccio (segue)

- L'Art. 24 del GDPR è una norma dal contenuto ampio che contiene i seguenti precetti:
  i) l'obbligo di mettere in atto misure che rendano ogni trattamento effettuato come conforme (*compliant*) alle previsioni del Regolamento;
  ii) l'obbligo che le misure adottate forniscano la garanzia (dimostrabile) di detta conformità;
  iii) l'obbligo di fondare la scelta delle misure adottate su preventive analisi dei rischi;
  iv) l'obbligo che la conformità così garantita sia anche facilmente dimostrabile (alle autorità competenti, ad eventuali altri organi ispettivi o giurisdizionali, o anche agli interessati al dato), di fatto individuando un vero e proprio obbligo di rendicontazione (i.e.: accountability).
- L'adozione di misure organizzative o di sicurezza ***dipenderà esclusivamente dalla scelta operata dal Titolare del trattamento o dal Responsabile***, sulla base di una valutazione (preventiva) il cui parametro sono le caratteristiche del trattamento effettuato: la sua natura, e quella dei tati cui si riferisce, il contesto, la finalità, i metodi e gli strumenti di trattamento, etc.
- La valutazione preventiva deve essere informata all'approccio basato sul rischio
- In sintesi, al Titolare del trattamento il GDPR chiede non più la previsione di specifiche misure di sicurezza ma l'individuazione ***di un vero programma di protezione del dato*** che si sostanzi nell'implementazione di processi non occasionali ma sistematici ed organizzati finalizzati al cd. *privacy management*

Il GDPR – concetti chiave e nuovo approccio (segue)

PRIVACY BY DESIGN

Le misure tecniche ed organizzative per la protezione dei dati anche di livello informatico vanno valutate nella fase di progettazione. Si segue, pertanto, l'idea del «prevenire non correggere»

Art 25.1 del GDPR

"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."*

PRIVACY BY DEFAULT

Per impostazione predefinita (i.e. di default), i titolari devono trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Occorre, quindi, progettare il sistema di trattamento garantendo la non eccessività dei dati raccolti.

Art. 25.2 del GDPR

«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»

Misure tecniche ed organizzative previste dal GDPR

Tra le nuove misure di sicurezza e organizzative che il titolare deve implementare, segnaliamo:

- Il registro delle attività di trattamento (anche Registro dei trattamenti o Registro)
- Designazione del Data privacy Officer (DPO) se necessario oppure opportuna
- Lo svolgimento della VIP (Valutazione Impatto Privacy), anche detta DPIA (Data protection Impact Asssment)
- Predisposizione di regolamentazione interna secondo i principi della privacy by design e privacy by default
- Notifica della violazione dei dati personali (data breach)

Data Privacy Officer - Art. 37 GDPR Designazione del Responsabile della Protezione dei dati

- Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:
  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 (sensibili, genetici, biometrici) o di dati relativi a condanne penali e a reati di cui all'articolo 10.
- Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.
- Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un **unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione**.
- (…)
- Il responsabile della protezione dei dati è designato in funzione delle **qualità professionali**, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.
- Il responsabile della protezione dei dati può essere un **dipendente** del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a **un contratto di servizi**.
- Il titolare del trattamento o il responsabile del **trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo** (comunicazione on line e modulistica).



Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 5 aprile 2017

Il Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO)

La scheda presenta la figura del Responsabile della protezione dei dati (RPD), o Data Protection Officer (DPO), in base a quanto previsto dal Regolamento (UE) 2016/679 e dalle Linee-guida del WP29

QUALI SONO I REQUISITI?

Il Responsabile della protezione dei dati, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

1. **possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze.
2. **adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse** . In linea di principio, ciò significa che il RPD non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali;
3. **operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio** (RPD/DPO esterno).

Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

IN QUALI CASI E' PREVISTO?

Dovranno designare obbligatoriamente un RPD:

a) amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;
b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
c) tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Anche per i casi in cui il regolamento non impone in modo specifico la designazione di un RPD, è comunque possibile una nomina su base volontaria.

Un gruppo di imprese o soggetti pubblici possono nominare un unico RPD.

QUALI SONO I COMPITI?

Il Responsabile della protezione dei dati dovrà, in particolare:

a) **sorvegliare l'osservanza del regolamento**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
b) collaborare con il titolare/responsabile, laddove necessario, nel condurre una **valutazione di impatto sulla protezione dei dati (DPIA)**;
c) **informare e sensibilizzare** il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
d) **cooperare con il Garante e fungere da punto di contatto per il Garante** su ogni questione connessa al trattamento;
e) **supportare** il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un **registro delle attività di trattamento** .

La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento. Per un quadro completo: www.garanteprivacy.it

Chi deve nominare un DPO?

Scheda Informativa del Garante

IN QUALI CASI E' PREVISTO?
Dovranno designare obbligatoriamente un RPD:

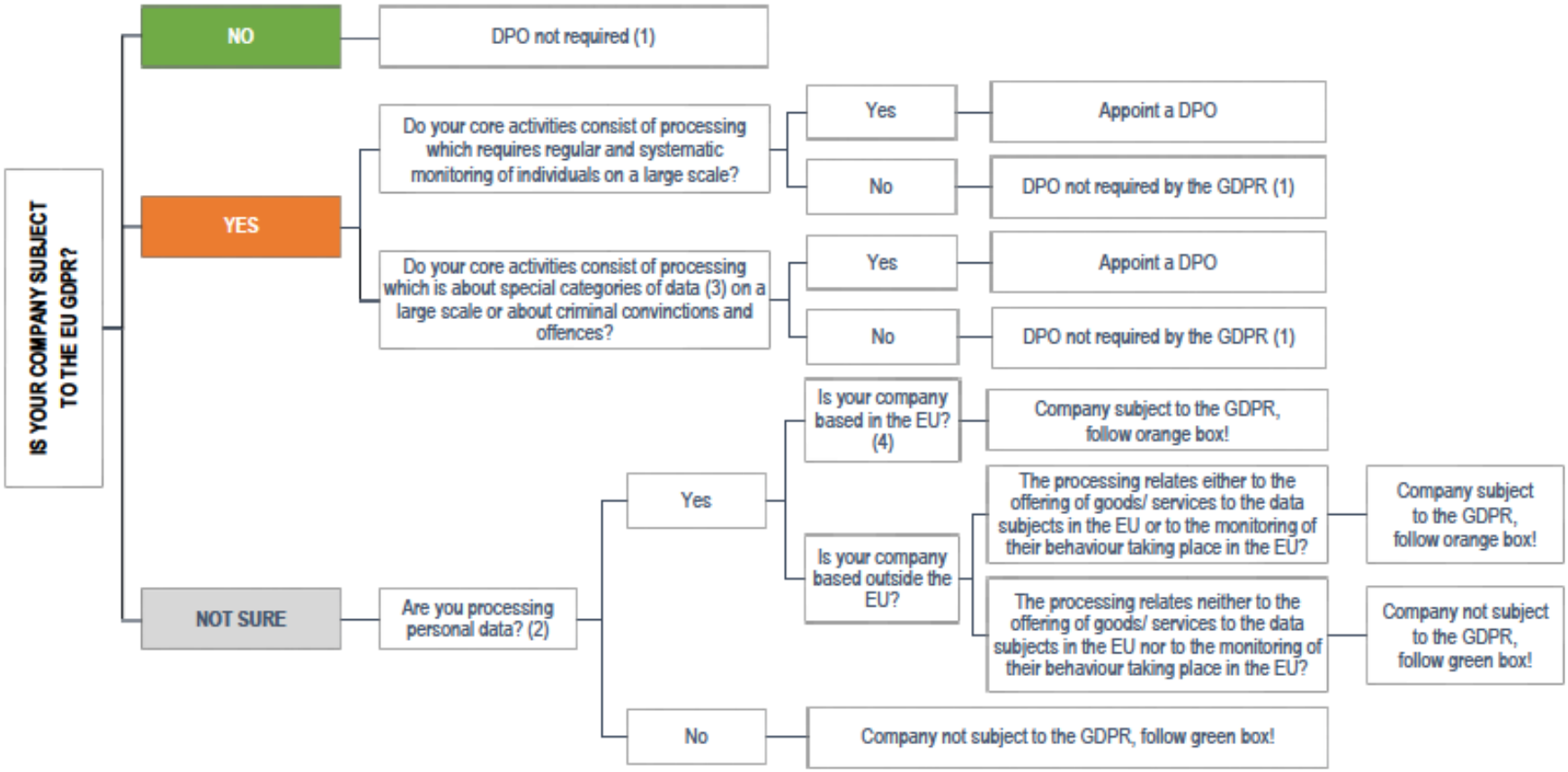
a) amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;
b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
c) tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Anche per i casi in cui il regolamento non impone in modo specifico la designazione di un RPD, è comunque possibile una nomina su base volontaria.

Un gruppo di imprese o soggetti pubblici possono nominare un unico RPD.

SHOULD YOUR COMPANY APPOINT A DATA PROTECTION OFFICER (DPO) UNDER THE EU GDPR?

DPO Network Europe
European Privacy Recruitment



(1) EU Member States may have / introduce other laws which require appointment of DPOs. Organizations may also opt to appoint DPOs even if there is no legal requirement at EU or Member State level. (2) For a definition of personal data, consult Article 4(1) of the EU GDPR. (3) For a definition of special categories of personal data, consult Article 9(1) of the EU GDPR. (4) See here list of EU Member States.

This document has been prepared for informational purposes only. The content of this document does not constitute legal advice and should not be relied upon as such. Consult your legal counsel when in any doubt about understanding your rights and obligations in order to comply with the law and regulations.

Legislazione Tecnica
Area Consulenza

Comunicazione dei dati di contatto del Responsabile della Protezione dei Dati - RPD (art. 37, par. 7 del Regolamento UE/2016/679 - RGPD)

A. Dati del soggetto che effettua la comunicazione

Cognome*[1] ..... Nome[1]* .....
E-mail[2] *: ..... Conferma E-mail *: .....
nella sua qualità di ☐ rappresentante legale o ☐ delegato del rappresentante legale
Cognome[3] ..... Nome[3] .....
☐ dichiara di aver preso visione dell'*informativa sul trattamento dei dati personali*
comunica i seguenti dati ai sensi e per gli effetti di cui all'art. 37, par. 7, del RGPD:

B. Dati del Titolare/Responsabile del trattamento

Il Titolare/Responsabile del trattamento è:

- ○ Censito nell'Indice nazionale dei domicili digitali delle imprese e dei professionisti *(www.inipec.gov.it - art. 6-bis Codice Amministrazione Digitale - D.Lgs n. 82/2005)*
- ○ Censito nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi *(www.indicepa.gov.it - art. 6-ter Codice Amministrazione Digitale - D.Lgs n. 82/2005)*
- ○ Non è censito in nessuno dei due precedenti indici

Denominazione *: .....
Codice Fiscale/P.IVA[4] *: ..... Soggetto privo di C.F./P.IVA ☐
Stato *: .....
Indirizzo[5] *: .....
CAP[6]*: ..... Città *: ..... Provincia[6]*: .....
Telefono *: .....
E-mail[7] *: .....
PEC[8] *: .....

Copia di cortesia. Consentito l'uso esclusivamente per la presente procedura. Non è consentito utilizzare il documento per la predisposizione di altre comunicazioni. La comunicazione deve essere effettuata esclusivamente utilizzando le procedure rese disponibili sulla sezione servizi online del sito del Garante. Non sono ammesse altre modalità.

I campi contrassegnati con * sono obbligatori salvo diversa o ulteriore indicazione
[1] Campo obbligatorio, salvo nel caso di autenticazione tramite SPID o CNS
[2] Indicare l'indirizzo di posta elettronica presso il quale si desidera ricevere il file che andrà firmato digitalmente
[3] Vengono richiesti (e sono obbligatori) solo se il soggetto di cui alla sezione A effettua la comunicazione su delega del rappresentante legale
[4] Dato obbligatorio. Nel caso non venga spuntato il campo "Soggetto privo di C.F./P.IVA" allora non è avvalorabile
[5] Da intendersi come residenza per le persone fisiche, Sede Legale per altri soggetti. Deve essere indicato l'indirizzo completo.
[6] Non compilabile se lo stato è diverso da "Italia"
[7] Campo obbligatorio solo se il Titolare/Responsabile dichiara di NON essere censito in uno dei due indici ex art. 6-bis o 6-ter del CAD, altrimenti è facoltativo
[8] Campo obbligatorio solo se il Titolare/Responsabile dichiara di essere censito in uno dei due indici ex art. 6-bis o 6-ter del CAD, altrimenti è facoltativo

Compiti affidati al DPO

Il GDPR fornisce compiti «minimi» al DPO. Il Titolare e il Responsabile possono affidarne di ulteriori nell'ambito del relativo incarico/nomina

Il DPO dovrà:

1) informare e fornire consulenza a titolare e al responsabile del trattamento nonché ai dipendenti degli obblighi derivanti dal regolamento;
2) sorvegliare l'osservanza del regolamento, nonché delle altre disposizioni europee o di diritto interno in materia di protezione dati;
3) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e attività di controllo;
4) fornire pareri e sorvegliare alla redazione del *Data Protection Impact Assessment* (c.d. DPIA);
5) fungere da punto di contatto e collaborare con l'Autorità Garante per la protezione dei dati personali;
6) controllare che le violazioni dei dati personali siano documentate, notificate e comunicate (c.d. Data Breach Notification Management).

Requisiti per diventare DPO

I titolari del trattamento devono designare come DPO un professionista con le seguenti caratteristiche:

- Possedere una conoscenza specialistica della normativa e delle prassi di gestione dei dati personali
- Essere in grado di adempiere alle proprie funzioni in piena indipendenza e in assenza di conflitti di interesse
- Operare come dipendente, oppure anche sulla base di un contratto di servizi.

Il titolare deve mettere a disposizione del DPO le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

Certificazioni

Allo stato attuale, non esistono titoli abilitanti o attestati formali che determinano l'idoneità di un DPO. Tuttavia, eventuali certificazioni delle competenze professionali rilasciate da enti indipendenti di terza parte costituiscono un valido strumento ai fini della verifica del possesso di un livello di conoscenza della disciplina. Tali certificazioni sono sempre volontarie, e non sono mai obbligatorie per svolgere il ruolo.

Albo dei DPO

Allo stato non esiste un Albo dei DPO

Posizione del DPO

- Il titolare dei dati e il responsabile assicurano che il DPO sia "tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali"
- E' essenziale che il DPO venga coinvolto quanto prima possibile in ogni questione attinente la protezione dei dati. Per quanto concerne le valutazioni di impatto sulla protezione dei dati, il regolamento prevede espressamente che il DPO vi sia coinvolto fin dalle fasi iniziali e specifica che il titolare ha l'obbligo di consultarlo nell'effettuazione di tali valutazioni
- Inoltre, è importante che il DPO sia annoverato fra gli interlocutori all'interno della struttura suddetta, e che partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento
- Il DPO non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti
- Il DPO riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile
- Il DPO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti

Conflitto di interessi del DPO

- Al DPO è consentito di "svolgere altri compiti e funzioni", ma a condizione che il titolare o il responsabile del trattamento si assicuri che "tali compiti e funzioni non diano adito a un conflitto di interessi".

- **L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza**. Anche se un DPO può svolgere altre funzioni, l'affidamento di tali ulteriori compiti e funzioni è possibile solo a condizione che essi non diano adito a conflitti di interessi (prevenzione e gestione del conflitto)

- **un DPO non può rivestire**, all'interno dell'organizzazione del titolare o del responsabile, **un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali**. Si tratta di un **elemento da tenere in considerazione caso per caso guardando alla specifica struttura organizzativa del singolo titolare o responsabile**.

Responsabilità del DPO

- Fermi restando i compiti del DPO, il controllo del rispetto del regolamento non significa che il RPD sia personalmente responsabile in caso di inosservanza.

- **Spetta, infatti, al Titolare, e non al DPO, mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR**

- **Il rispetto delle norme in materia di protezione dei dati fa parte della responsabilità d'impresa del titolare del trattamento**.

Applicazione del GDPR agli Ordini professionali di livello nazionale e territoriale

- Gli Ordini sono sottoposti alla normativa privacy di cui al GDPR, in quanto:
  - ✓ enti pubblici non economici
  - ✓ organismi di diritto pubblico
  - ✓ gestori di banche dati
- Gli Ordini perseguono fini istituzionali e, nell'ambito dei fini istituzionali, non soggiacciono al regime dei consensi relativamente ai dati che obbligatoriamente vanno forniti (cfr. legge istitutiva della professione)
- Gli Ordini, relativamente ai dati ulteriori devono ottenere specifici consensi
- L'applicazione della normativa privacy è una competenza del Consiglio dell'Ordine (quale Titolare del trattamento)
- Altri soggetti interni sono tenuti ad un'adeguata conoscenza della normativa privacy (Segreteria dell'Ordine; Consiglio di disciplina; Commissioni dell'Ordine; Consulenti e collaboratori)

Suggerimenti pratici: cosa fare entro il 25 maggio

- Prendere coscienza che il termine del 25 maggio è un termine ultimo di adeguamento
- Il Titolare del trattamento deve verificare che il trattamento effettuato sia conforme ai principi privacy (liceità, trasparenza, minimizzazione dei dati)
- Il Titolare deve verificare la conformità della propria documentazione (Consensi/informativa) alla nuova normativa di riferimento
- Il Titolare del trattamento deve predisporre il Registro dei trattamenti
- Il Titolare deve svolgere un risk assessment (valutazione di probabilità di accadimento/valutazione di impatto) finalizzato alla predisposizione di idonee misure di sicurezza, anche alla luce di quelle già esistenti
- Deve essere definita una governance interna: chi fa cosa, titolare/responsabile/DPO
- Il Titolare deve nominare un DPO
- Il Titolare, unitamente al DPO, deve verificare la necessità di una VPI
- Il Titolare dee adottare procedure interne di gestione del data breach, portabilità, diritto all'oblio
- Il Titolare dee adottare una privacy policy che fissi i principi per l'adempimento degli obblighi di protezione dei dati

Grazie per l'attenzione!

Rosalisa Lancia
Legislazione Tecnica
r.lancia@legislazionetecnica.it
www.legislazionetecnica.it

©Copyright Legislazione Tecnica 2018
Il presente materiale didattico è di proprietà di Legislazione Tecnica. La riproduzione, la copiatura, l'adattamento totale o parziale e con qualsiasi mezzo, nonché la memorizzazione elettronica, sono riservati per tutti i Paesi