G. L. RABITA - A. PEDICONE

INVESTIGAZIONI PRIVACY HANDBOOK

-

Guida all'applicazione Privacy per le Agenzie Investigative
in base al Nuovo Reg. EU 679/2016 e D. Lgs. 10 agosto 2018 n. 101

EDIZIONE LEONARDO INTELLIGENCE

PRIVACY HANDBOOK

-

Guida all'applicazione Privacy per le Agenzie Investigative
in base al Nuovo Reg. EU 679/2016 e D. Lgs. 10 agosto 2018 n. 101

Autori: G.L.Rabita - A. Pedicone

Ia edizione 19 Settembre 2018

Indice

_____

INTRODUZIONE pag. 4

La nomina di un RPD *pag. 5*
L'istituzione di un Registro dei Trattamenti *pag. 6*
Le nomine *pag. 7*
L'implementazione delle misure di sicurezza *pag. 8*
La comunicazione del Data Breach *pag. 10*

Il nuovo D. Lgs. 10 agosto 2018 n. 101 pag. 11

Categorie particolari di dati *pag. 11*
Le sanzioni *pag. 13*
Cosa adeguare in aggiornamento al nuovo DL 101/2018 *pag. 14*
1. Aggiornare l'informativa privacy da allegare all'incarico investigativo *pag. 14*
2. Le nomine interne all'agenzia *pag. 15*
3. Le nomine esterne all'agenzia *pag. 15*
4. Aggiornare l'informativa privacy del sito web *pag. 15*
5. Aggiornare l'informativa privacy nelle mail in uscita *pag. 15*
6. Elaborare un documento delle misure di sicurezza impiegate *pag. 16*
7. Il registro dei trattamenti di cui all'art. 30 del GDPR *pag. 16*

CONCLUSIONI pag. 16

Bibliografia pag. 18

Sitografia pag. 18

INTRODUZIONE

Come noto oggi, 19 settembre 2018, entra in vigore il D. Lgs. 10 agosto 2018 n. 101[1], che adegua la normativa italiana a quella europea in materia di circolazione e protezione dei dati personali.

Bisogna ricordare che il Nuovo Regolamento Privacy UE 679/2016[2] è considerato completamente assorbito dal 24 maggio 2018 e i due anni antecedenti hanno permesso a tutti di adeguarsi. Il Garante Privacy Italiano in questi due anni ha dato delle linee guida per capire cosa va adeguato all'interno delle aziende, enti, organizzazioni e amministrazione pubblica. Nel corso del tempo queste linee guida sono cambiate, anche perché, capire come far assorbire in Italia un cambiamento così importante non è cosa facile.

I cambiamenti più importanti introdotti dal Nuovo Regolamento EU 679/2016 sono sicuramente:

a) la nomina di un RPD;

b) l'istituzione di un Registro dei Trattamenti;

c) le nomine;

d) l'implementazione dei sistemi di sicurezza;

e) la comunicazione del Data Breach.

---

1 DECRETO LEGISLATIVO 10 agosto 2018, n. 101
Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018)
note: Entrata in vigore del provvedimento: 19/09/2018

2 REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=EN

La nomina di un RPD

La nomina di un RPD non è una cosa immediata e non è consigliabile rivolgersi a chiunque. È consigliabile invece valutare bene chi ricoprirà il ruolo, le competenze effettive in materia di privacy e la conoscenza approfondita del settore di riferimento.

Il Garante da grande importanza a questa figura e nel regolamento EU 679/2016 ne evidenzia i requisiti e i compiti[3]:

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.
2. 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.
3. 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;
4. operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio (RPD/DPO esterno);
5. sorvegliare l'osservanza del regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
6. collaborare con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);
7. 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;
8. cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;
9. 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 .

3 https://www.garanteprivacy.it/regolamentoue/rpd

L'istituzione di un Registro dei Trattamenti

Il registro è la cosa che certificherà che i trattamenti sono stati eseguiti secondo il nuovo regolamento. Su questo argomento è bene soffermarsi un attimo in più perché impostare un registro dei trattamenti non è una cosa immediata.

Tutti sono tenuti ad avere un registro dei trattamenti, eccetto, recita il codice, gli organismi con meno di 250 dipendenti. Seppur vero che, la gran parte delle agenzie investigative sono piccole aziende che non arrivano a 250 dipendenti, è da tener presente che, le agenzie investigative hanno una specifica di attività che è sicuramente definibile a rischio, secondo quanto prescritto dall'art.30 § 5 del GDPR EU 679/2016[4]. Ma sopratutto, l'attività professionale dell'investigatore privato rientra senza dubbio in quanto viene descritto dall'art.9 § 3.[5]

Nello specifico, il citato art.9 § 3, dice che: i dati personali sensibili possono essere trattati solo sotto la responsabilità di un professionista soggetto al *segreto professionale* o da altra persona anch'essa soggetta all'*obbligo di segretezza*[6]. Questa fattispecie si addice indiscutibile al tipo di trattamento con cui si confronta l'investigazione privata, è evidente quindi, l'obbligatorietà per l'investigatore privato e/o l'agenzia investigativa di istituire un registro dei trattamenti.

Il Garante indica il registro dei trattamenti[7] come strumento fondamentale, non soltanto ai fini dell'eventuale controllo, ma anche come efficace strumento aziendale (o per l'ente pubblico) per disporre di un quadro aggiornato dei dati a disposizione, dei trattamenti effettuati e/o per lo sviluppo di un'analisi del rischio.

In ultimo, ma non per importanza, il GDPR 679/2016 impone che il registro debba avere forma scritta, o anche elettronica, e debba essere esibito su richiesta del Garante.

---

4 Articolo 30 EU RGPD "Registri delle attività di trattamento"
5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

5 Articolo 9 EU RGPD "Trattamento di categorie particolari di dati personali"
3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

6 Nel caso di specie l'investigatore privato.

7 https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili#registro

Le nomine

Cosa si intende per nomine? Il Nuovo Regolamento EU 679/2016 prevede una figura di cui abbiamo già parlato, l'RPD – Responsabile Protezione Dati, ma c'è un'altra figura denominata Responsabile[8] che non centra niente con l'RPD.

Il Responsabile del trattamento è una figura nominata dal Titolare del trattamento per compiti specifici. Il Responsabile del trattamento deve mettere in atto tutte quelle misure tecniche e organizzative che garantiscano i requisiti del regolamento e la tutela dei diritti dell'interessato.

Esempio pratico. Per ogni agenzia investigativa arriva il momento che un caso richieda l'ausilio di un consulente tecnico. Il consulente in questione entrerà in contatto con dati che riguardano l'indagine e che sono stati affidati in sede di mandato. Il consulente non ha un contratto che lo leghi al mandante ma di fatto conosce parte dei dati, se non tutti i dati, che riguardano il suo caso. L'agenzia investigativa dovrà nominare, specificatamente Responsabile del trattamento, il consulente in questione.

La nomina di un Responsabile del trattamento è un vero e proprio contratto regolamentato dall'art.28 § 3 del GDPR EU 679/2016[9], che deve contenere:

- la durata del trattamento
- la natura e la finalità del trattamento
- il tipo di dati personali
- le categorie di interessati
- gli obblighi e i diritti del titolare del trattamento.

Inoltre, la nomina, secondo il codice, deve avere formule di garanzie specifiche, quali:

a) il responsabile deve trattare i dati soltanto su istruzione documentata del titolare del trattamento;

b) impegno alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

---

8 Articolo 28 EU RGPD "Responsabile del trattamento"
1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

9 Articolo 28 EU RGPD "Responsabile del trattamento"
3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

c) il responsabile adotti tutte le misure richieste ai sensi dell'articolo 32[10];

d) rispetti le condizioni nel caso nomini un sub-responsabile;

e) assista il titolare del trattamento con misure tecniche e organizzative adeguate;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 32;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali;

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie.

Quindi, per formulare le nomine, bisogna prima capire chi fa cosa all'interno dell'agenzia investigativa, dopodiché, sarà bene far sottoscrivere un vero e proprio contratto di nomina che contenga tutte le specifiche e le garanzie previste dal GDPR.

L'implementazione delle misure di sicurezza

Per parlare di sicurezza dobbiamo partire da un concetto su cui il GDPR mette un forte accento, responsabilità (accountability)[11]. Non basta più avere misure minime di sicurezza ma è necessario adeguare le misure a: tecnico-organizzative adeguate.

Diventa quindi responsabilità diretta del Titolare del trattamento, e dei suoi Responsabili, capire che misure di sicurezza adottare in totale autonomia, ammesso che, queste siano adeguate.

Cercando di rendere tutto più chiaro e semplice, diciamo che: l'agenzia investigativa sicuramente ha a che fare con informazioni importanti che non possono e non devono essere divulgate. Non vogliamo che le informazioni di un servizio investigativo o di sicurezza vengano sottratte o accidentalmente perse o distrutte.

Il primo passo da fare è chiedersi: c'è la possibilità che le informazioni relative ad un cliente, il registro degli

---

10 Articolo 32 EU RGPD "Sicurezza del trattamento"
1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

11 Articolo 24 EU RGPD "Responsabilità del titolare del trattamento"
1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

affari, le risultanze di un indagine, vengano rubate, perse, artefatte, visionate accidentalmente da persone non autorizzate? Se questo accadesse che tipo di rischio ci sarebbe per i diritti e la libertà dell'interessato?

Da qui, il Titolare decide in autonomia le misure di sicurezza che reputa idonee. È da sottolineare misure di sicurezza e non sistemi di sicurezza. C'è una differenza sostanziale. Il GDPR non vuole che si metta solo un allarme in più o qualche telecamera di sorveglianza, ma, che si valuti di implementare:
- la qualità di conservazione dei dati
- la cifratura dei dati conservati
- la definizione specifica dei ruoli all'interno dell'organizzazione
- la formazione del personale sul trattamento
- implementazione delle procedura di gestione dei dati
- la policy di sicurezza informatica
- mantenere gli aggiornamenti software
- il tracciamento delle operazioni di trattamento
- la sicurezza fisica (porte blindate, telecamere, allarmi, controllo accessi…).

Se un trattamento avesse argomentazioni particolari con rischi importanti, ci sarà bisogno di un'analisi preventiva, che il GDPR chiama *valutazione di impatto*[12]. O meglio, la domanda da porsi sarà: che tipo di problemi potrebbero abbattersi sull'interessato del trattamento in caso di incidente?

Con questo tipo di *rischio elevato*, prima di procedere al trattamento, il Titolare dovrà elaborare un valutazione di impatto e comunicarla, sempre in via preventiva, al Garante. Su come preparare una valutazione di impatto, in quali casi è prevista e quando comunicarla, rimandiamo all'ottima guida sul sito istituzionale del Garante Privacy[13] sull'individuazione e gestione del rischio.

In caso di controllo da parte dell'Autorità Garante, verrà valutata con estrema serietà la valutazione del rischio fatta e le misure di sicurezza messe in opera. Saranno ovviamente sanzionate tutte quelle situazioni non considerate idonee.

---

12 Articolo 35 EU RGPD "Valutazione d'impatto sulla protezione dei dati"
1. 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. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

13 https://www.garanteprivacy.it/regolamentoue/DPIA/gestione-del-rischio

La comunicazione del Data Breach

Il Data Breach è semplicemente la notifica delle violazioni di dati personali. O meglio. Le misure di sicurezza hanno fallito, l'incidente imprevisto può capitare, i dati dei clienti sono andati persi, distrutti, rubati, devo comunicarlo immediatamente al Garante.

Per chiarezza riportiamo quanto scritto, molto bene, sul sito istituzionale del Garante[14]:

> *A partire dal 25 maggio 2018, tutti i titolari – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all´autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, la notifica all´autorità dell´avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell´art. 34, che coincidono solo in parte con quelle attualmente menzionate nell´art. 32-bis del Codice. I contenuti della notifica all´autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli artt. 33 e 34 del regolamento. Si segnalano, al riguardo, le linee-guida in materia di notifica delle violazioni di dati personali del Gruppo "Articolo 29", qui disponibili www.garanteprivacy.it/regolamentoue/databreach.*
>
> *RACCOMANDAZIONI*
>
> *Tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all´autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda art. 33, paragrafo 5); tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall´art. 32-bis, comma 7, del Codice. Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.*

14 https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili

IL NUOVO D. Lgs. 10 agosto 2018 n. 101

Il decreto legislativo 101/2018 parla esattamente di:"*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018)*".[15]

Questo decreto legislativo molto atteso, chiamato gergalmente decreto di assorbimento nazionale della norma europea, risolve una serie di dubbi sull'applicazione, in Italia, del Nuovo Regolamento Privacy EU.

Categorie particolari di dati

È da notare l'attenzione del legislatore italiano, nel redirigere questo decreto, dedicata a quei settori dove il trattamento dei dati personali è complesso, delicato e caratterizzato da fattispecie particolari. Il legislatore ha previsto varie disposizioni a completamento degli artt. 9[16] e 10[17] del GDPR EU 679/2016, consentendo il trattamento in una serie di particolarità. Più precisamente il D.L. 101/2018[18], adeguandosi al Regolamento EU, cambia in *categorie particolari di dati* quei dati che, fino al 25 maggio 2018, venivano espressi nel D.L. 196/2003[19] come *dati sensibili* e *dati giudiziari*.

Nel nuovo decreto legge 101/2018 è inoltre previsto un potere specifico del Garante nell'emanare provvedimenti biennali relativi a misure di garanzia per il trattamento di dati genetici, biometrici e relativi alla salute dell'interessato. I provvedimenti biennali avranno l'obiettivo di dare nuove indicazioni aggiornate sui trattamenti e direttive di adeguamento delle misure di sicurezza.

Il decreto legge 101/2018 si occupa anche di specificare nel dettaglio i casi di trattamento di dati relativi a condanne penali, reati, dati trattati per un accertamento e/o per l'esercizio della difesa di un diritto in sede

15 DECRETO LEGISLATIVO 10 agosto 2018, n. 101 - Entrata in vigore del provvedimento: 19/09/2018
http://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg

16 Articolo 9 EU RGPD "Trattamento di categorie particolari di dati personali"

17 Articolo 10 EU RGPD "Trattamento dei dati personali relativi a condanne penali e reati"

18 DECRETO LEGISLATIVO 10 agosto 2018, n. 101 (GU n.205 del 4-9-2018)
Art. 22 Altre disposizioni transitorie e finali 2. A decorrere dal 25 maggio 2018 le espressioni «dati sensibili» e «dati giudiziari» utilizzate ai sensi dell'articolo 4, comma 1, lettere d) ed e), del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, ovunque ricorrano, si intendono riferite, rispettivamente, alle categorie particolari di dati di cui all'articolo 9 del Regolamento (UE) 2016/679 e ai dati di cui all'articolo 10 del medesimo regolamento.

19 Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" pubblicato nella Gazzetta Ufficiale n. 174 del 29 luglio 2003 - Supplemento Ordinario n. 123.

giudiziaria. Ed in particolare l'art. 2-octies comma 3[20], per quanto di interesse alle agenzie investigative, precisa che:

Fermo quanto previsto dai commi 1 e 2, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza e' consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, riguardanti, in particolare:

a) l'adempimento di obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dagli articoli 9, paragrafo 2, lettera b), e 88 del regolamento;

b) l'adempimento degli obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali;

c) la verifica o l'accertamento dei requisiti di onorabilita', requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;

d) l'accertamento di responsabilita' in relazione a sinistri o eventi attinenti alla vita umana, nonche' la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attivita' assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;

e) l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

f) l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;

g) l'esecuzione di investigazioni o le ricerche o la raccolta di informazioni per conto di terzi ai sensi dell'articolo 134 del testo unico delle leggi di pubblica sicurezza;

20 DECRETO LEGISLATIVO 10 agosto 2018, n. 101 (GU n.205 del 4-9-2018)
Art. 2-octies (Principi relativi al trattamento di dati relativi a condanne penali e reati).

Le sanzioni

Nel nuovo D.L. 101/2018, molte disposizioni limitano senza dubbio gli ambiti di trattamento di dati per *categorie particolari* ma ne precisano le fattispecie. Per esempio, in tema di delitti per il trattamento illecito di dati personali in *categorie particolari*, si rilevano tre specie: dolo specifico, di profitto e di danno cagionato a terzi. È sottolineare che il termine *delitti* si riferisce a condotte illecite e fatti gravi che riguardano esclusivamente il trattamento di dati di *categorie particolari* in violazione degli artt. 2-septies[21] e 2-octies[22] del decreto.

Se la violazione, su fatti gravi, legata al trattamento di dati di *categorie particolari* è oggetto di trattamento su larga scala, le conseguenze sono molto gravi, art.15 D.L. coma 1/c 101/2018[23], con condanne fino a sei anni.

c) dopo l'articolo 167, sono inseriti i seguenti:

«Art. 167-bis (Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala). - 1. Salvo che il fatto costituisca piu' grave reato, chiunque comunica o diffonde al fine di trarre profitto per se' o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, e' punito con la reclusione da uno a sei anni.

2. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine trarne profitto per se' o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, e' punito con la reclusione da uno a sei anni, quando il consenso dell'interessato e' richiesto per le operazioni di comunicazione e di diffusione.

3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.».

«Art. 167-ter (Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala). - 1. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine trarne profitto per se' o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala e' punito con la reclusione da uno a quattro anni.

---

21 DECRETO LEGISLATIVO 10 agosto 2018, n. 101 (GU n.205 del 4-9-2018)
Art. 2-septies (Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute)

22 DECRETO LEGISLATIVO 10 agosto 2018, n. 101 (GU n.205 del 4-9-2018)
Art. 2-octies (Principi relativi al trattamento di dati relativi a condanne penali e reati)

23 DECRETO LEGISLATIVO 10 agosto 2018, n. 101 (GU n.205 del 4-9-2018)
Art. 15 Modifiche alla parte III, titolo III, del decreto legislativo 30 giugno 2003, n. 196

Cosa adeguare in aggiornamento al nuovo DL 101/2018

Dopo tutte le valutazioni introduttive, vediamo i principali e più comuni obblighi in adeguamento per le agenzie di investigazioni, indipendentemente dai punti di attività previsti DM 269/2010[24] all'art.5.[25]

1. Aggiornare l'informativa privacy da allegare all'incarico investigativo.

Redarre una nuova informativa privacy, secondo i dettami del GDPR e DL 101/2019, che andrà a sostituire la precedente. La nuova informativa deve essere consegnata ai clienti, dipendenti, collaboratori, i quali devono esprimere esplicito consenso.

---

24 DECRETO 1 dicembre 2010, n. 269
Regolamento recante disciplina delle caratteristiche minime del progetto organizzativo e dei requisiti minimi di qualita' degli istituti e dei servizi di cui agli articoli 256-bis e 257-bis del Regolamento di esecuzione del Testo unico delle leggi di pubblica sicurezza, nonche' dei requisiti professionali e di capacita' tecnica richiesti per la direzione dei medesimi istituti e per lo svolgimento di incarichi organizzativi nell'ambito degli stessi istituti. (11G0036) (GU n.36 del 14-2-2011 - Suppl. Ordinario n. 37)
note: Entrata in vigore del provvedimento: 16/03/2011

25 DECRETO 1 dicembre 2010, n. 269
Art. 5 Qualita' dei servizi di investigazione privata e di informazione commerciale 1. Ai fini della definizione delle tipologie di attivita', di cui all'articolo 4, comma 2, e dei requisiti minimi di qualita' dei servizi, sono individuate le seguenti tipologie di attivita' d'indagine, esercitata nel rispetto della legislazione vigente e senza porre in essere azioni che comportino l'esercizio di pubblici poteri, riservate agli organi di Polizia ed alla magistratura inquirente:
a) investigazione privata
a.I): attivita' di indagine in ambito privato, volta alla ricerca ed alla individuazione di informazioni richieste dal privato cittadino, anche per la tutela di un diritto in sede giudiziaria, che possono riguardare, tra l'altro, gli ambiti familiare, matrimoniale, patrimoniale, ricerca di persone scomparse;
a.II): attivita' di indagine in ambito aziendale, richiesta dal titolare d'azienda ovvero dal legale rappresentante o da procuratori speciali a cio' delegati o da enti giuridici pubblici e privati volta a risolvere questioni afferenti la propria attivita' aziendale, richiesta anche per la tutela di un diritto in sede giudiziaria, che possono riguardare, tra l'altro: azioni illecite da parte del prestatore di lavoro, infedelta' professionale, tutela del patrimonio scientifico e tecnologico, tutela di marchi e brevetti, concorrenza sleale, contraffazione di prodotti;
a.III): attivita' d'indagine in ambito commerciale, richiesta dal titolare dell'esercizio commerciale ovvero dal legale rappresentante o da procuratori speciali a cio' delegati volta all'individuazione ed all'accertamento delle cause che determinano, anche a livello contabile, gli ammanchi e le differenze inventariali nel settore commerciale, anche mediante la raccolta di informazioni reperite direttamente presso i locali del committente;
a.IV): attivita' di indagine in ambito assicurativo, richiesta dagli aventi diritto, privati e/o societa' di assicurazioni, anche per la tutela di un diritto in sede giudiziaria, in materia di: dinamica dei sinistri, responsabilita' professionale, risarcimenti sul lavoro, contrasto dei tentativi di frode in danno delle societa' di assicurazioni;
a.V): attivita' d'indagine difensiva, volta all'individuazione di elementi probatori da far valere nell'ambito del processo penale, ai sensi dell'articolo 222 delle norme di coordinamento del codice di procedura penale e dall'articolo 327-bis del medesimo Codice;
a.VI): attivita' previste da leggi speciali o decreti ministeriali, caratterizzate dalla presenza stabile di personale dipendente presso i locali del committente. Per lo svolgimento delle attivita' di cui ai punti da a.I), a.II), a.III) e a.IV) i soggetti autorizzati possono, tra l'altro, svolgere, anche a mezzo di propri collaboratori segnalati ai sensi dell'articolo 259 del Regolamento d'esecuzione TULPS: attivita' di osservazione statica e dinamica (c.d. pedinamento) anche a mezzo di strumenti elettronici, ripresa video/fotografica, sopralluogo, raccolta di informazioni estratte da documenti di libero accesso anche in pubblici registri, interviste a persone anche a mezzo di conversazioni telefoniche, raccolta di informazioni reperite direttamente presso i locali del committente.
b) informazioni commerciali:
b.I): attivita', richiesta da privati o da enti giuridici pubblici e privati, di raccolta, analisi, elaborazione, valutazione e stima di dati economici, finanziari, creditizi, patrimoniali, industriali, produttivi, imprenditoriali e professionali delle imprese individuali, delle societa' anche di persone, persone giuridiche, enti o associazioni nonche' delle persone fisiche, quali, ad esempio, esponenti aziendali, soci, professionisti, lavoratori, parti contrattuali, clienti anche potenziali dei terzi committenti, nel rispetto della vigente normativa nazionale e comunitaria in materia di tutela della privacy.

Il consenso[26], deve essere secondo finalità e non deve rientrare nel corpo contrattuale, secondo quanto previsto dall'art. 7 del GDPR EU 679/2016.

Sarebbe consigliabile adeguare informativa e consenso anche dei dipendenti/collaboratori già assunti ancora in servizio e di quei clienti con incarichi ancora aperti. Potrebbe essere utile affiggere una copia dell'informativa in sala d'attesa, sala riunioni, o comunque, in un locale dell'ufficio di comune utilizzo.

2. Le nomine interne all'agenzia.

Avendo chiaro chi fa cosa nell'agenzia investigativa, elaborare una nomina che specifichi i compiti, di *Responsabile del Trattamento* e di eventuali *Sub Responsabili del Trattamento*, per i dipendenti e i collaboratori.

3. Le nomine esterne all'agenzia.

Avendo chiaro chi fa cosa per l'agenzia investigativa, elaborare una nomina che specifichi i compiti di tutte quelle figure che collaborano esternamente, quali *Responsabili del Trattamento* e di eventuali *Sub Responsabili del Trattamento*, tipo: commercialisti, consulenti del lavoro, gestori del sito internet, medici del lavoro e ogni altra figura esterna alla quale sono forniti per via telematica o cartacea dati personali di interessati.

4. Aggiornare l'informativa privacy del sito web.

Cosa da non sottovalutare! Elaborare una nuova informativa che tenga conto dei dati raccolti anche in termini di cookies gestiti da terze parti (es. Google Analytics che vi dice quanto visitatori avete sul sito) e la policy di raccolta dati personali, se sul sito è presente un form per l'invio di richieste e/o domande.

5. Aggiornare l'informativa privacy nelle mail in uscita.

Altro argomento da non sottovalutare. È bene comunicare in calce, nelle proprie email di agenzia utilizzando

---

26 Articolo 7 EU RGPD "Condizioni per il consenso"
1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

una email istituzionale e non una personale, una propria informativa sul trattamento dei dati, privacy policy, e le avvertenze su un illecito trattamento dei dati trasmessi e raccolti.

6. Elaborare un documento delle misure di sicurezza impiegate.

Abbiamo avuto modo di parlare di misure di sicurezza e di quanto sia importante impiegare le misure di sicurezza adeguate che dimostrino la responsabilità (accountabily) del *Titolare del trattamento*.

Sarà bene quindi valutare internamente tutte le misure da mettere in opera e elaborare un documento che spieghi il cosa si è deciso di impiegare e perché, a tutela dei dati raccolti o che si raccoglieranno, degli interessati e, in caso di perdita/sottrazione, cosa si intende fare per la tutela degli interessati e per procedura di tempestiva comunicazione al Garante.

7. Creare il registro dei trattamenti di cui all'art. 30 del GDPR.

Per chi non abbia già provveduto alla creazione del registro dei trattamenti entro il 25 maggio 2018, sarà bene farlo subito, con l'entrata in vigore del DL 101/2018. Un modello del registro dei trattamenti è disponibile sul sito del Garante.[27]

CONCLUSIONI

Il Garante per la Protezione dei Dati Personali - GPDP - è sensibile ad un bellissimo concetto introdotto dal nuovo codice europeo, il **Privacy by Design**[28], o meglio, ogni realtà ha delle sue specifiche e chi meglio delle associazioni di categoria conosce le necessità del proprio settore. Il Garante esorta all'autoregolamentazione di settore per la specificità di alcuni trattamenti, ed è possibile chiedere al Garante formule specifiche per il settore di riferimento.

Nello specifico il GDPR EU 679/2016 Articolo 25 recita:

> *"Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"*
>
> *1. 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*

27 https://www.garanteprivacy.it/regolamentoue/registro
28 Articolo 25 EU RGPD "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"

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.

2. 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.

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

La Leonardo Intelligence, associazione di categoria per le investigazioni e la sicurezza, ha già messo a in opera, da marzo 2018, una serie di iniziative a sostegno dei propri associati in merito a:
- la nomina di un RPD-DPO per le agenzie investigative associate;
- un registro dei trattamenti specifico per le agenzie investigative;
- formazione e aggiornamento sul Nuovo Regolamento EU 67872016;
- modello di nomina di Responsabile del trattamento specifico per agenzie investigative;
- valutazione di impatto;
- adeguamento delle misure di sicurezza.

Per chiarimenti, modifiche e/o integrazioni info@leonardointelliegcne.it.

Autori

G. L. Rabita

Tenente dei Carabinieri in congedo
Socio Fondatore della Leonardo Intelligence
Docente Univ. di Scienze Investigative e della Sicurezza
Docente di Metodologie e Tecniche Investigative
Perito iscritto all'Albo del Trib. Ord. di Roma Sez. Penale
Titolare dell'Istituto Investigativo Leon Rabi
RPD-DPO e Consulente Privacy per il settore investigativo

A. Pedicone

Consigliere per gli Studi Legislativi - Leonardo Intelligence
Titolare dell'Agenzia Investigativa "Andrea Pedicone & Partners"
Già Docente dell'Università di Messina
Già Docente dell'Università del Molise
Già Docente dell'Università Sapienza di Roma
Investigatore di fiducia dell'Associazione Nazionale Forense
RPD-DPO e Consulente Privacy per il settore investigativo

Bibliografia

REGIO DECRETO 18 giugno 1931, n. 773
Approvazione del testo unico delle leggi di pubblica sicurezza. (031U0773) (GU n.146 del 26-6-1931 - Suppl. Ordinario n. 146)
note: Entrata in vigore del provvedimento: 11/07/1931

Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" pubblicato nella Gazzetta Ufficiale n. 174 del 29 luglio 2003 - Supplemento Ordinario n. 123.

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

DECRETO LEGISLATIVO 10 agosto 2018, n. 101
Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018)
note: Entrata in vigore del provvedimento: 19/09/2018

Sitografia

---

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=EN

https://www.garanteprivacy.it

http://www.gazzettaufficiale.it/atto/stampa/serie_generale/originario

http://www.camera.it/parlam/leggi/deleghe/03196dl.htm

www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1931-06-18;773!vig=