IfinSistemi
Conservatore Accreditato AgID

IfinConsulting

GIUGNO 2019

IfinConsulting News

IN ARRIVO I PRIMI CONTROLLI E LE SANZIONI PER VIOLAZIONE DELLA PRIVACY

A distanza di otto mesi dall'entrata in vigore del D.lgs 101/2018 che ha adeguato la normativa nazionale alle disposizioni del Regolamento UE 2016/679 (di seguito "GDPR"), il 19 maggio è scaduto il cosiddetto "periodo di grazia" ossia il termine per adeguarsi alla nuova disciplina sulla privacy.

Dal 20 maggio chi non si è adeguato alle disposizioni del GDPR sulla protezione dei dati rischia di essere sanzionato severamente. Occorre ricordare che l'applicazione delle sanzioni previste dall'art. 166 del Codice Privacy e dall'art. 83 del GDPR non è, comunque, un atto automatico.

L'effettiva irrogazione di una sanzione, a seguito di una contestazione (reclamo, segnalazione o controllo d'ufficio) di violazione del GDPR, è preceduta dal procedimento istruttorio, le cui modalità di svolgimento sono definite dal provvedimento 1/2019 del **Garante Privacy** (rappresenta l'organo competente ad irrogare le sanzioni). Il Regolamento 1/2019 si applica, in particolare, ai procedimenti:

- di trattazione di reclami delle aziende, proposti ai sensi dell'art. 142 del Codice Privacy;
- di esame di segnalazioni, ossia qualsiasi richiesta diretta a sollecitare un controllo del Garante sul rispetto della normativa;
- di svolgimento di controlli e ispezioni ai sensi degli artt. 157 e 158 del Codice Privacy che l'Autorità Garante può avviare d'ufficio per verificare possibili violazioni della disciplina rilevante, anche nel contesto dell'attività di revisione sulla protezione dei dati personali avviata a seguito della convocazione del titolare o del responsabile presso l'unità organizzativa competente dell'Autorità. In particolare, le attività ispettive possono essere delegate alla Guardia di Finanza o svolte avvalendosi della collaborazione di altri organi dello Stato.

La durata dei procedimenti istruttori è fissata dal Regolamento 2/2019 concernente l'individuazione dei termini e delle unità organizzative responsabili dei procedimenti amministrativi presso il Garante per la protezione dei dati personali.

Nel caso in cui non sia previsto alcun termine, il procedimento deve concludersi entro 90 giorni dalla ricezione della relativa istanza.

Come verranno accertati gli inadempimenti e chi è responsabile delle violazioni

Sono circa 90 gli adempimenti richiesti per adeguarsi alla disciplina sulla protezione dei dati personali. Tali adempimenti sono rimessi alla responsabilità del Titolare del trattamento che deve dimostrare di essere "accountable", cioè di aver adottato, tutte le pratiche interne (processo di adeguamento), affinché il trattamento sia effettuato in conformità al GDPR.

È bene inoltre evidenziare che, il Titolare del trattamento può delegare terzi nella gestione dei dati: il Responsabile del trattamento (nel GDPR data processor) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del Titolare del trattamento. Il Titolare del trattamento conserva il potere decisionale, è colui che decide il motivo e le modalità del trattamento, ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa.

I "ritardatari" rischiano sanzioni che possono raggiungere i 200 milioni di euro o il 4% del fatturato.

All'interno del GDPR è presente un margine di discrezionalità circa la possibilità di infliggere una sanzione e la determinazione dell'importo della stessa. I criteri di valutazione adottati, per esprimere un giudizio su un eventuale inadempienza alle prescrizioni in materia di privacy, tengono conto dei seguenti aspetti:

SOMMARIO

- la natura, gravità e durata della violazione;
- il carattere doloso o colposo della violazione;
- il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attuarne i possibili effetti negativi.

Con riferimento al secondo criterio, le valutazioni verranno effettuate sulla base di elementi oggettivi, tuttavia il Working Party ha provveduto ad illustrare alcune condotte che potranno integrare il suddetto carattere doloso. Queste sono riconducibili alle ipotesi di:

- trattamenti illeciti autorizzati esplicitamente dal senior management, ovvero ignorando i pareri formulati dal DPO;
- modifica di dati personali, avente la finalità di fornire un'impressione "fuorviante" circa il conseguimento degli obiettivi individuati;
- vendita di dati, in mancanza di verifica e/o ignorando la scelta liberamente esercitata dagli interessati.

Le sanzioni in materia di protezione dei dati personali

Il GDPR disciplina le ipotesi per cui è prevista l'applicazione di sanzioni amministrative pecuniarie e/o penali. Per quanto riguarda le prime, esse possono raggiungere i 10 milioni di euro o, se superiore, il 2% del fatturato mondiale nei casi ad esempio:

- di violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione;
- di trattamento illecito di dati personali che non richiede l'identificazione dell'interessato;
- di mancata o errata notificazione e/o comunicazione di un data breach all'Autorità nazionale competente;
- di violazione dell'obbligo di nomina del DPO;
- di mancata applicazione di misure di sicurezza.

L'importo delle sanzioni amministrative pecuniarie può salire fino a 20 milioni di euro, o alternativamente, sino al 4% del fatturato mondiale dell'impresa nei casi di seguito elencati, a titolo esemplificativo:

- inosservanza di un ordine, di una limitazione provvisoria o definitiva concernente un trattamento, imposti da un'autorità nazionale competente;
- trasferimento illecito cross-border di dati personali ad un destinatario in un paese terzo.

Infine, l'autorità di controllo ha il potere di irrogare sanzioni correttive che possono consistere in:

- avvertimenti al titolare o al responsabile del trattamento sul fatto che i trattamenti previsti possono violare le norme;
- ammonimenti al titolare o al responsabile del trattamento ove i trattamenti abbiano violato le norme;
- ordinare al titolare o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i relativi diritti;
- ordinare al titolare o al responsabile del trattamento di conformare i trattamenti alle norme, specificando eventualmente le modalità e i termini per la conformità;
- imporre una limitazione provvisoria o definitiva al trattamento, sospendere temporaneamente il trattamento, o vietare del tutto;
- ordinare la rettifica, la cancellazione o l'aggiornamento dei dati personali;
- revocare le certificazioni o ingiungere all'organismo di certificazione di ritirare le certificazioni rilasciate se i requisiti non sono soddisfatti;
- infliggere le sanzioni amministrative pecuniarie;
- ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

Conclusioni

Da una breve analisi delle prime sanzioni amministrative, riguardo a inadempimenti al GDPR, emerge chiaramente che l'approccio utilizzato dalle Autorità di Controllo dei singoli stati in Europa, non è quello di punire eccessivamente i titolari ma attenersi al principio principe della ragionevolezza: se la violazione è minore e la sanzione pecuniaria dovesse rappresentare un onere sproporzionato per una persona fisica, allora si opta nell'applicare un ammonimento. Tuttavia, in ogni caso si deve tenere conto della tipologia, della gravità e alla durata della violazione, del carattere doloso, delle misure adottate per attenuare il danno subito, al livello di responsabilità, a eventuali precedenti violazioni ed eventuali altri fattori aggravanti o attenuanti.

L'obiettivo è garantire un'applicazione graduale e progressiva del regolamento europeo e di guidare le organizzazioni verso questo percorso.

GESTIONE DOCUMENTALE E CONSERVAZIONE DIGITALE NELL'AMBITO DELLA TRACCIABILITA' RIFIUTI

Con l'approvazione il 7 febbraio scorso del decreto "Semplificazioni", il legislatore ha previsto l'istituzione del "Registro elettronico nazionale per la tracciabilità dei rifiuti", che sarà controllato direttamente dal Ministero dell'Ambiente e della Tutela del Territorio e del Mare e andrà a sostituire il SISTRI, abolito dall'1 gennaio 2019.

A questo nuovo registro dovranno iscriversi:

- enti e imprese che trattano rifiuti;
- produttori di rifiuti pericolosi;
- enti e imprese che raccolgono o trasportano rifiuti pericolosi a titolo professionale;
- commercianti ed intermediari di rifiuti pericolosi;
- consorzi istituiti per il recupero e il riciclaggio di particolari tipologie di rifiuti;
- i soggetti previsti all'articolo 189, comma 3 del D.lgs. 152/2006 per quanto riguarda i rifiuti non pericolosi.

Il termine di iscrizione sarà individuato da un successivo decreto, che sarà emanato da parte del Ministro dell'ambiente e della tutela del territorio e del mare, insieme al Ministro dell'economia e delle finanze, di concerto con il Ministro dello sviluppo economico, il Ministro per la pubblica amministrazione e il Ministro delle infrastrutture e dei trasporti.
Sempre per opera del Ministero dell'Ambiente verranno indicate le modalità di organizzazione e funzionamento del Registro elettronico nazionale.
Dal 1° gennaio 2019 e fino alla piena operatività del Registro elettronico nazionale, la tracciabilità dei rifiuti è garantita provvedendo alla tenuta e alla compilazione dei registri di carico e scarico, dei formulari di identificazione dei rifiuti (FIR) per il trasporto degli stessi, e alla trasmissione annuale del MUD (modello unico di dichiarazione ambientale) (artt.188-189-190 e 193 del d.lgs. 152/2006). Inoltre, l'art. 194-bis del d.lgs. 152/2006 dispone che, in attuazione delle disposizioni del Codice dell'amministrazione digitale e per consentire la lettura dei dati riportati, gli obblighi relativi alle modalità di compilazione e tenuta del registro di carico e scarico e del formulario di trasporto dei rifiuti (FIR) possono essere effettuati in formato digitale.

Per quanto riguarda il registro di carico e scarico, la sua gestione può essere ricondotta a quella dei registri IVA, il richiamo alla sua gestione che prevede numerazione, vidimazione e gestione come tali registri, la troviamo all'art. 190 del Testo unico ambientale. Inoltre, bisogna ricordare che l'art. 2215 bis del Codice Civile afferma che *"i libri, i repertori, le scritture e la documentazione la cui tenuta è obbligatoria per disposizione di legge o di regolamento o che sono richiesti dalla natura dell'impresa possono essere formati e tenuti con strumenti informatici. (...) Gli obblighi di numerazione progressiva, vidimazione e gli altri obblighi previsti dalle disposizioni di legge o di regolamento per le tenuta dei libri, repertori e scritture, ivi compreso quello di regolare tenuta dei medesimi, sono assolti, in caso di tenuta con strumenti informatici, mediante apposizione, ogni tre mesi a far data dalla messa in opera, della marcatura temporale e della firma digitale dell'imprenditore, o di altro soggetto del medesimo delegato, inerenti al documento contenente le registrazioni relative ai tre mesi precedenti. (...) I libri, i repertori e le scritture tenuti con strumenti informatici, secondo quanto previsto dal presente articolo, hanno l'efficacia probatoria di cui agli articoli 2709 e 2710 del codice civile"*.

Pertanto, il registro di carico e scarico dei rifiuti può a tutti gli effetti essere formato digitalmente e inserito nella normativa IVA.
Naturalmente, per essere un documento informatico legalmente valido, deve seguire un *iter* ben preciso: deve esserci l'apposizione della firma e della marca temporale, per garantire l'autenticità, l'integrità e l'autore del documento; il numero di protocollo che lo identifica deve essere generato automaticamente dal sistema e deve essere registrato in modo immodificabile, lo stesso dicasi per i numeri delle registrazioni al suo interno; i processi di gestione devono essere realizzati in modo da garantire la leggibilità dei documenti e la loro fruibilità, per quanto riguarda la sua conservazione, i registri di carico e scarico dovranno essere versati in un sistema di conservazione e secondo un *modus operandi* che rispetti le regole tecniche espresse dal DPCM 3 dicembre 2013, rispettando le tempistiche dettate per i documenti fiscalmente rilevanti.

Un po' più complessa la questione applicata ai formulari (FIR) perché le indicazioni relative alla forma del modello che deve descrivere il formulario risultano difficilmente sostituibili in un documento digitale; questo perché il DM del 1 aprile 1998, riportante il regolamento per la definizione del modello e dei contenuti del formulario di accompagnamento dei rifiuti (FIR), indica che i formulari devono essere stampati su carta idonea, numerati progressivamente anche con l'adozione di prefissi alfabetici di serie e predisposti soltanto dalle tipografie autorizzate dal Ministero delle Finanze.
Quindi, fermo restando che anche per i FIR la possibilità di ricorrere ai documenti digitali è permessa dall'art.2215 bis del Codice civile, ad oggi per quanto riguarda questa specifica tipologia documentaria mancano tecniche specifiche che ne permettano la sua trasposizione su supporto digitale.

Va detto che il Testo unico ambientale (l'articolo 194-bis, c.3) prevede la possibilità di trasmettere la quarta copia del formulario via PEC, ma non ne precisa le modalità. In assenza di un decreto ministeriale attuativo dell'articolo 194-bis, la disciplina cui fare riferimento è oggi rappresentata dal DLgs marzo 2005, n.82, che regola la trasmissione e la conservazione dell'informazione in modalità digitale.

Si può affermare che in questo modo è iniziata la semplificazione della tracciabilità dei dati ambientali. Semplificazione che è comunque facoltativa, poiché l'invio mediante PEC è ammesso, ma non imposto.

NODO SMISTAMENTO ORDINI (NSO): INVIO TELEMATICO DEI DOCUMENTI DI ORDINE DEGLI ENTI DEL SERVIZIO SANITARIO NAZIONALE

Con il Nodo Smistamento Ordini il Dipartimento della Ragioneria di Stato del Ministero dell'economia e delle finanze ha dato il via ad un sistema digitale di trasmissione documenti che è integrato con la Banca Dati Nazionale dei Contratti Pubblici e con lo SDI, ovvero il Sistema di interscambio.
Il sistema è stato creato dopo l'emanazione della Legge di Bilancio 2018, che descriveva questo strumento con il fine di garantire la trasparenza negli approvvigionamenti delle amministrazioni pubbliche, tenendo sotto controllo in primis gli acquisti e le spese delle aziende pubbliche sanitarie nazionali. L'intenzione di applicare tale sistema alle aziende sanitarie viene ribadito anche dal DL 7 dicembre 2018 del Ministero dell'economia e della finanza, che fissa l'entrata in vigore dell'obbligo di adozione del NSO da parte delle aziende sanitarie il 1° ottobre 2019. Da questa data l'obbligo scatterà anche per gli loro intermediari e i fornitori delle aziende sanitarie.
Insieme al Decreto legge, che introduce l'NSO dando indicazioni per il suo utilizzo, bisogna tenere con anche delle linee guida della Ragioneria di Stato dello scorso 15 marzo 2019 e rilasciate nella versione completa del 9 maggio.
Con l'avvio del Nodo smistamento ordini dal prossimo 1° ottobre 2019 i soggetti obbligati alla sua adozione dovranno dismettere i precedenti canali di trasmissione dei documenti relativi agli ordini e, per quanto riguarda le fatture connesse ai vari ordini, bisogna tenere conto che dovranno necessariamente contenere al loro interno i riferimenti dell'ordine cui si riferiscono, altrimenti le amministrazioni pubbliche non potranno liquidarle.
Il Nodo di Smistamento degli ordini avrà, come nel caso delle fatture elettroniche che transitano per il Sistema di Interscambio, un formato prestabilito. Nel caso del NSO, il legislatore ha deciso di adottare l'UBL XML, standard internazionale per la creazione dei documenti digitali, anziché il più noto XML, utilizzato per lo SDI. Questo messaggio che transiterà per il Nodo sarà composto dal documento contenente i dati utili per l'ordine, come per esempio le indicazioni sul tipologia e sulla quantità dei prodotti o dei servizi acquistati, insieme ad una sorta di busta di trasmissione, un file contenente le indicazioni relative al mittente e al destinatario.
Dopo la creazione del messaggio, questo verrà inviato al Nodo Smistamento Ordini attraverso gli stessi canali che sono stati già attivati per la fatturazione elettronica, vale a dire i canali web service e di interoperabilità e la PEC. In particolare va sottolineato che in caso di impiego della PEC, il documento va inviato all'indirizzo nso@pec.sogei.it.
Una differenza rispetto alla fatturazione elettronica sta nella possibilità di impiegare Peppol, il progetto europeo che mira ad uniformare i processi dell'e-procurement, e che nel nostro Paese è già usato per ordini, DDT e fatture nella Regione Emilia Romagna.
Un'ultima indicazione, l'ordine può essere di quattro differenti tipi:

- l'ordine emesso dal cliente, vale a dire l'azienda pubblica del Servizio Sanitario Nazionale, verso il fornitore;
- l'ordine pre-concordato, che viene spedito dal fornitore all'amministrazione pubblica;
- l'ordine risposta, che consente al fornitore di accettare, rifiutare o modificare l'ordine fatto dall'amministrazione pubblica;
- l'ordine di riscontro, che consente all'amministrazione pubblica di confermare, rifiutare o sostituire risposte con modifiche o ordini concordati inviati dalle aziende fornitrici.

Con questo sistema si percepisce l'intenzione legislativa e tecnica di sviluppare la digitalizzazione nel mondo sanitario.

I SERVIZI DI IFINCONSULTING

Consulenza
Consulenza normativa.
Consulenza archivistica e archivistico-informatica.
Redazione di documenti (atti di nomina del responsabile della conservazione e del responsabile del trattamento dei dati personali) di pareri e di contratti.
Verifica della rispondenza alle prescrizioni normative (Audit).
Supporto per il conseguimento dell'accreditamento presso AgID.
Servizi di consulenza e supporto alle aziende che vogliono implementare sistemi di gestione certificabili.
Supporto alla qualificazione SaaS per Cloud della PA.

Formazione
Corsi sulla dematerializzazione (ambito privato, pubblico e settore clinico).
Corsi sulla fatturazione elettronica B2G e B2B.
Corsi di formazione del responsabile della conservazione.

IFIN SISTEMI srl a socio unico
PADOVA . MILANO . ROMA .

PD. Via G. Medici 9/A 35138
Tel. 049.5001500
Fax 049.5001692
www.ifin.it
www.conservazionesostitutiva.it