issn 1591-9544 vol. 19 n. 60 (1-2 - 2018) Estratto

Ciberspazio e Diritto

Rivista Internazionale di Informatica Giuridica

Periodico quadrimestrale

Il GDPR: una nuova era per la protezione dei dati?

Direttore
Giovanni Ziccardi
Professore Associato di Informatica Giuridica - Università degli Studi di Milano

Comitato Scientifico e Referees

Paolo Becchi
Università degli Studi di Genova

Nerina Boschiero
Università degli Studi di Milano

Albina Candian
Università degli Studi di Milano

Maria Teresa Carinci
Università degli Studi di Milano

Pasquale Costanzo
Università degli Studi di Genova

Francesco Delfini
Università degli Studi di Milano

Paolo Di Lucia
Università degli Studi di Milano

Diana-Urania Galetta
Università degli Studi di Milano

Alberto Maria Gambino
Università Europea di Roma

Mario G. Losano
Università del Piemonte Orientale

Luca Lupária
Università di Roma Tre

Claudio Luzzati
Università degli Studi di Milano

Giovanni Pascuzzi
Università degli Studi di Trento

Lorenzo Picotti
Università degli Studi di Verona

Dianora Poletti
Università di Pisa

Oreste Pollicino
Università Bocconi

Giovanni Sartor
Università degli Studi di Bologna

Vito Velluzzi
Università degli Studi di Milano

STEM Mucchi Editore

Ciberspazio e Diritto

Rivista Internazionale di Informatica Giuridica

Informatica Giuridica
Diritti di Libertà e Dissidenza Digitale
Investigazioni Digitali

Rivista quadrimestrale

Vol. 19, n. 60 (1-2 - 2018)

STEM Mucchi Editore

Direzione e Redazione: Prof. Avv. Giovanni Ziccardi c/o
Amm.ne: STEM Mucchi Editore - Via Emilia est, 1741 41122 Modena

Autorizzazione del Tribunale di Modena, n. 1507 del 10/12/1999

issn 1591-9544

© STEM Mucchi Editore - Società Tipografica Editrice Modenese Srl
Via Emilia est, 1741 - 41122 Modena
info@mucchieditore.it
www.mucchieditore.it
facebook.com/mucchieditore
twitter.com/mucchieditore
instagram.com/mucchi_editore

La legge 22 aprile 1941 sulla protezione del diritto d'Autore, modificata dalla legge 18 agosto 2000, tutela la proprietà intellettuale e i diritti connessi al suo esercizio. Senza autorizzazione sono vietate la riproduzione e l'archiviazione, anche parziali, e per uso didattico, con qualsiasi mezzo, del contenuto di quest'opera nella forma editoriale con la quale essa è pubblicata. Fotocopie per uso personale del lettore possono essere effettuate nel limite del 15% di ciascun volume o fascicolo di periodico dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941 n. 633. Le riproduzioni per uso differente da quello personale potranno avvenire solo a seguito di specifica autorizzazione rilasciata dall'editore o dagli aventi diritto.

Vol. 19 n. 60 (1-2 - 2018)
Impaginazione STEM Mucchi (MO), stampa Legodigit (TN)

Finito di stampare nel mese di luglio del 2018

Ciberspazio e Diritto

Direttore

Prof. Avv. **Giovanni Ziccardi**, Facoltà di Giurisprudenza, Univ. degli Studi di Milano

Comitato Scientifico

Paolo Becchi, Università di Genova; **Nerina Boschiero**, Università di Milano; **Albina Candian**, Università di Milano; **Maria Teresa Carinci**, Università di Milano; **Pasquale Costanzo**, Università di Genova; **Francesco Delfini**, Università di Milano; **Paolo Di Lucia**, Università di Milano; **Diana-Urania Galetta**, Università di Milano; **Alberto Maria Gambino**, Università Europea di Roma; **Mario G. Losano**, Università del Piemonte Orientale "Amedeo Avogadro" (Alessandria); **Luca Lupária**, Università di Roma Tre; **Claudio Luzzati**, Università di Milano; **Giovanni Pascuzzi**, Università di Trento; **Lorenzo Picotti**, Università di Verona; **Dianora Poletti**, Università di Pisa; **Oreste Pollicino**, Università Bocconi; **Giovanni Sartor**, Università di Bologna; **Vito Velluzzi**, Università di Milano.

Comitato Editoriale

Angelica Bonfanti, Università di Milano; **Fabio Bravo**, Università di Bologna; **Raffaella Brighi**, Università di Bologna; **Roberto Caso**, Università di Trento; **Rossella Cerchia**, Università di Milano; **Corrado del Bò**, Università di Milano; **Roberto Flor**, Università di Verona; **Letizia Mancini**, Università di Milano; **Monica Palmirani**, Università di Bologna; **Giovanni Pellerino**, Università di Lecce; **Pierluigi Perri**, Università di Milano; **Francesca Poggi**, Università di Milano; **Giovanni Maria Riccio**, Università di Salerno, **Andrea Rossetti**, Università di Milano Bicocca; **Margherita Salvadori**, Università di Torino; **Stefania Stefanelli**, Università di Perugia; **Stefano Zanero**, Politecnico di Milano.

Comitato redazionale

Giulia Escurolle; Silvia Martinelli; Michele Martoni; Samanta Stanco; Gabriele Suffia.

Informazioni per gli abbonati

L'abbonamento decorre dal 1 gennaio di ogni anno e dà diritto a tutti i numeri dell'annata, compresi quelli già pubblicati. Il pagamento può essere effettuato direttamente all'editore tramite bonifico intestato a STEM Mucchi Editore (IT IT92E0760112900000011051414 - SWIFT/BIC:BPPIITRRXX), a ricevimento fattura (valido solo per enti e società), mediante carta di credito (sottoscrivendo l'abbonamento on line all'indirizzo www.mucchieditore.it, oppure precisando numero, scadenza e data di nascita). Al fine di assicurare la continuità nell'invio dei fascicoli, gli abbonamenti si intendono rinnovati per l'anno successivo. La disdetta dell'abbonamento va effettuata tramite raccomandata a/r alla sede della Casa editrice entro il 31 dicembre dell'annata in corso. I fascicoli non pervenuti all'abbonato devono essere reclamati al ricevimento del fascicolo successivo. Decorso tale termine si spediscono, se disponibili, dietro rimessa dell'importo (prezzo di copertina del fascicolo in oggetto). Le annate arretrate sono in vendita al prezzo della quota di abbonamento dell'anno in corso. Si accordano speciali agevolazioni per l'acquisto di più annate arretrate, anche non consecutive, della stessa rivista. Per l'acquisto di singoli fascicoli della rivista consultare il catalogo online all'indirizzo www.mucchieditore.it. Il cliente ha la facoltà di recedere da eventuali ordini unicamente mediante l'invio di una lettera raccomandata a/r alla sede della Casa editrice, o e-mail (seguita da una raccomandata a/r) entro le successive 48 ore atte a consentire l'identificazione del cliente e dell'ordine revocato (merce, data, luogo, etc.). La revoca dell'ordine deve essere spedita entro e non oltre il 10° giorno successivo alla data di sottoscrizione.

Abbonamento annuo **(3 numeri, iva inclusa)**
Italia € 72,00 - Cartaceo + Digitale € 85,00 - Cartaceo + Digitale IP € 92,00
Estero € 86,00 - Cartaceo + Digitale € 99,00 - Cartaceo + Digitale IP € 106,00
Versione digitale € 56,00 - Digitale IP € 65,00

Ogni fascicolo cartaceo € 24,00 + spese di spedizione
Ogni fascicolo digitale € 20,00

La fruizione dei contenuti digitali avviene tramite la piattaforma www.torrossa.it

Per maggiori informazioni si rimanda alla Sezione Periodici di www.mucchieditore.it

Rivista soggetta a doppia peer-review

Codice etico della Rivista e procedura di Review

La qualità scientifica dei lavori pubblicati è assicurata da una procedura di revisione (c.d. peer review), attuata secondo principi di trasparenza, autonomia e indiscusso prestigio scientifico dei revisori.

- Il lavoro è sottoposto a un esame preliminare da parte del Direttore, del Comitato di Redazione o di un loro componente delegato, per rilevare la sua attinenza alle caratteristiche e ai temi propri della rivista, nonché l'eventuale presenza di evidenti e grossolane carenze sotto il profilo scientifico.
- Il successivo referaggio consiste nella sottoposizione del lavoro alla valutazione di due professori esperti nella materia, italiani o stranieri, scelti dalla direzione nell'ambito di un comitato di *referees* o, in casi eccezionali, inerenti alla specificità dell'argomento trattato, all'esterno dello stesso.
- Il sistema di referaggio è quello c.d. doppio cieco (*double blind peer review*): lo scritto è inviato ai due revisori in forma anonima. All'autore non sono rivelati i nomi dei revisori. I revisori sono vincolati a tenere segreto il loro operato e si impegnano a non divulgare l'opera e le relative informazioni e valutazioni, che sono strettamente confidenziali: l'accettazione preventiva di questo vincolo e di questo impegno è precondizione per assumere il compito di referaggio.
- I nomi dei revisori consultati per la valutazione dei lavori pubblicati dalla rivista nel corso dell'anno sono pubblicati in apposito elenco nell'ultimo fascicolo dell'annata senza riferimento ai lavori valutati.
- I revisori invieranno alla direzione (o al componente delegato), la proposta finale, che può essere di: accettazione dello scritto per la pubblicazione (eventualmente con un lavoro di editing); accettazione subordinata a modifiche migliorative, sommariamente indicate dal revisore (in questi casi lo scritto è restituito all'autore per le modifiche da apportare); non accettazione dello scritto per la pubblicazione.
- I revisori, nel pieno rispetto delle opinioni degli autori e a prescindere dalla condivisione del merito delle tesi da essi sostenute, dovranno

tenere in specifica considerazione l'originalità e l'utilità pratica delle idee espresse nel lavoro, nonché la conoscenza delle fonti pertinenti, la consapevolezza culturale, la consistenza critica del percorso argomentativo e la correttezza formale.

- La direzione della rivista ha la responsabilità ultima della decisione di pubblicazione o meno del contributo, ferma restando la esclusiva responsabilità dell'autore per il suo contenuto e le opinioni in esso manifestate.

Ciberspazio e Diritto n. 60 (1-2 - 2018), in questo numero:

GDPR e blockchain

GDPR tra sicurezza, responsabilizzazione e certificazioni

Ciberspazio e diritto, vol. 19, n. 60 (1-2 - 2018), pp. 245-263

Luci ed ombre del regime delle diverse tipologie di certificazione previste dal GDPR – General Data Protection Regulation

Giovanna Raffaella Stumpo*

Sommario: 1. Premessa. – 2. Il SGP: Sistema di Gestione Privacy e rilevanza della certificazione. – 3. Significato, tipologie e iter di certificazione: cosa non dice il Regolamento. – 3.1. La certificazione di sistema ed informazioni esplicative nel Regolamento. – 4. La certificazione delle competenze: il disposto del Regolamento e la norma tecnica UNI 11007. – 4.1. I requisiti di qualificazione tecnica della figura del DPO (*Data Protection Officer*).

1. *Premessa*

Dal 25 maggio il GDPR (General Data Protection Regulation) – Regolamento del Parlamento europeo e del Consiglio 27 aprile 2016 n. 697 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati) (anche solo il Regolamento) – è vincolante ed efficace per i 28 Stati Membri (SM) dell'Unione Europea, con efficacia abrogativa della Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

In virtù della sua diretta applicabilità, il Regolamento comporta per tutti i diversi Operatori di mercato dell'UE (Aziende, P.A. e Studi) che, nell'esercizio del business ed in particolare nell'attività di produzione / erogazione di beni /servizi trattano dati personali di interessati – persone fisiche – con ricorso in tutto/in parte a strumenti elettronici e non (cfr. Capo I art. 2 comma 1 del Regolamento), e con impatto in ambito UE (cfr. Capo I, art. 3 del Regolamento) e che si qualificano quali titolari del trattamento ai sensi dell'art. 4, punto 7) della normativa UE, l'obbligo di realizzare un SGP "Sistema di Gestione Privacy", in linea previsionale certificabile a cura di Ente terzo accreditato.

* Avvocato del Foro di Milano, Giornalista pubblicista, Formatore, Esperto in discipline strumentali all'esercizio della professione forense, Auditor SGQ e Certificazione ISO 9001 e Auditor M.O.G. ex D.Lgs. n. 231/2001.

Sul punto, è infatti chiaro il disposto del "considerando 100" del Regolamento, a norma del quale «al fine di migliorare la trasparenza ed il rispetto del presente Regolamento dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli e marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi».

Il meccanismo di certificazione preso in considerazione dal Regolamento rimanda pertanto al mondo delle c.d. norme internazionali e tecniche sui sistemi di gestione, come parametro su cui impostare un SGP - Sistema di Gestione Privacy per l'allineamento organizzativo e tecnico ai suoi precetti, e con possibile relativa certificazione a cura di Ente terzo accreditato, utile a fini di trasparenza informativa e per l'onere della prova imposto al titolare, di conformità alla c*ompliance* normativa.

Sotto diverso profilo – e quanto al diverso tema della "certificazione delle competenze", il meccanismo rileva per la non meno importante dimostrazione che il titolare deve fornire rispetto a "formazione, capacità e competenza" prescritte dal Regolamento, in relazione ad alcune figure rilevanti dell'"Organigramma privacy".

Vediamo meglio di cosa stiamo parlando, individuando anche le principali lacune previsionali del Regolamento sul sistema delle certificazioni.

2. *Il SGP: Sistema di Gestione Privacy e rilevanza della certificazione*

Salve le eccezioni espressamente previste per alcuni adempimenti (in particolare per le PMI) per previsione del Regolamento, a chi, all'interno dell'Organizzazione effettua le determinazioni circa "finalità e mezzi del trattamento" – e, quindi, conseguentemente si qualifica quale titolare-, è fatto obbligo "di responsabilizzazione" (cfr. Capo II, art. 5 comma 2 del Regolamento); con onere di un comportamento attivo, che sul piano organizzativo, tecnico e di metodo, deve rispondere ai seguenti principi ispiratori:

- *accountability* (i.e. necessità di dimostrare l'adozione di politiche privacy e misure adeguate alla tutela dei diritti dell'interessato, in conformità al dettato regolamentare);

- *privacy by design* (i.e. necessità di adozione di misure tecnico – organizzative adeguate a protezione dei dati oggetto del trattamento da parte del titolare, fin dalla progettazione ed anche nell'atto del trattamento);
- *privacy by default* (i.e. necessità in capo al titolare di garantire che i dati vengano trattati solo per finalità previste e per il tempo strettamente necessario a tali finalità).

Per essere *compliant* operativamente, al titolare il Regolamento richiede di "mettere a sistema" gli adempimenti imposti a tutela dei diritti e delle libertà degli interessati coinvolti nelle attività di trattamento dei dati, correlati alle attività di business; adottando in chiave preventiva misure tecnico – organizzativo adeguate – anche riguardo ai profili della sicurezza – ai possibili rischi sottesi ad ogni trattamento.

Di più e con l'obiettivo di favorire al massimo la libera circolazione dei dati nelle transazioni UE in un clima di fiducia e di fidatezza da parte degli interessati, il Regolamento fa obbligo al titolare di fornire la prova delle sue effettive capacità tecnico – organizzative in rispondenza ai requisiti imposti a tutela degli interessati ed in coerenza ai requisiti di normativa cogente; rischiando in difetto di ciò – il titolare –, di incorrere in sanzioni amministrative pecuniarie particolarmente rilevanti e che possono anche arrivare fino ad un massimo di 20 milioni di euro / fino al 4% del fatturato mondiale totale annuo (cfr. Capo VIII, art. 83 del Regolamento).

In tema di SGP – Sistema di Gestione Privacy, rileva in particolare il disposto dell'art. 24, commi I e II del Regolamento, a norma dei quali: «1. Tenuto conto della natura, dell'ambito di applicazione, del contenuto 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.

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento».

L'onere della prova per il titolare di essere *compliant* con i requisiti del SGP – Sistema di Gestione Privacy a fronte della cogenza normativa,

è previsto al comma 3 dell'art. 24[1] del Regolamento; che sul punto introduce una sorta di "presunzione di conformità", là ove prevede che: «3. L'adesione ai codici di condotta di cui all'art. 40 o a un meccanismo di certificazione approvato di cui all'art. 42, può essere utilizzato come elemento per dimostrare il rispetto degli obblighi imposti al titolare».

Il tema è ulteriormente stressato e ribadito dal disposto dell'art. 25 del Regolamento come segue: «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 sono oggetto del 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.

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».

Tralasciando in questa sede la trattazione dei codici di condotta, quanto al tema della certificazione rileva nel Regolamento il disposto

[1] Per il caso in cui il titolare scelga di avvalersi della figura del responsabile del trattamento di cui all'art. 28 del Regolamento, vale parallelamente il disposto del comma 5 del predetto articolo, a norma del quale: «L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'art. 40 o a un meccanismo di certificazione approvato di cui all'art. 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai par. 1 e 4 del presente articolo».

dell'art. 42 comma 1. A norma del quale, tenute in considerazione le specifiche esigenze delle PMI, per tutti gli altri diversi Operatori di mercato:

«1. Gli SM, la autorità di controllo, il comitato e la Commissione incoraggiano in particolare, a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati, nonché di sigilli e marchi di protezione di dati, allo scopo di dimostrare la conformità al presente Regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento».

Con queste previsioni il Regolamento fa quindi un importante rimando alla normazione internazionale di natura volontaria e tecnica che regolamenta il sistema delle certificazioni. Strumento rilevante nella materia *"de quo",* a vantaggio del titolare, a fini sia di comunicazione esterna nei confronti dei Clienti e degli Stakeholders, sia probatori; essendo che un Sistema di Gestione certificato può fungere da strumento "di fidatezza" quanto al corretto trattamento dei dati; ed anche quale possibile esimente avanti l'A.G., analogamente a quanto vale per l'Organizzazione che scelga di dotarsi si un M.O.G. (Modello Organizzativo Gestionale) *ex* D.lgs. n. 231/2001.

3. *Significato, tipologie e iter di certificazione: cosa non dice il Regolamento*

Per "certificazione", ai sensi della norma tecnica ed internazionale UNI CEI EN 45020:1998 (Normazione ed attività connesse) s'intende l'attestazione fornita da un soggetto indipendente ed autonomo (rispetto all'Organizzazione ed al di lui Cliente) in forma di "assicurazione scritta" che un prodotto/servizio o un processo, è conforme ai requisiti specificati da una previsione di natura tecnica di riferimento (i.e. uno standard).

Più nel dettaglio, la certificazione consiste in una attestazione rilasciata da un Organismo terzo, autonomo ed indipendente dall'Operatore di mercato, circa l'idoneità di un prodotto/servizio/un processo a rispondere a requisiti di conformità di cui ad uno standard tecnico di riferimento, ovvero della capacità della struttura e delle persone della struttura a realizzare il business per tramite di processi interni organizzati "in modo sistemico" e a gestirli "con modalità controllate", nel rispetto di requisiti espressi dallo standard tecnico di riferimento.

Più precisamente:

- la certificazione di prodotto/servizio: è una forma di "assicurazione diretta", con cui si accerta la rispondenza di un prodotto tangibile/ intangibile ai requisiti della norma tecnica applicabile;
- la certificazione di sistema: assicura la capacità di un'Organizzazione (produttrice di beni o erogatrice di servizi) di strutturarsi e gestire le proprie risorse ed i propri processi gestionali, produttivi ed erogativi in modo da riconoscere e soddisfare i bisogni dei Clienti, impegnandosi al miglioramento continuo della sua "prestazionalità". È una forma di "assicurazione indiretta" e riguarda in particolare: i) i SGQ - Sistema di Gestione per la Qualità (ISO 9001); ii) i SGR - Sistema di Gestione del Rischio (ISO 31000); iii) i SGA - Sistema di Gestione per l'Ambiente (ISO 14001); iii) i SGSI - Sistema di Gestione per la Sicurezza delle Informazioni (ISO 27001); iv) i SGSA - Sistema di Gestione per la Sicurezza Alimentare (ISO 22000); v) i SG SSLL - Sistemi di Gestione per la Salute e Sicurezza nei luoghi di lavoro (OHSAS 18001:2007); vi) i SGBC - Sistema di Gestione per la Business Continuity (ISO 22301); vii) i SGAN - Sistema di Gestione anticorruzione (ISO 37001) etc.[2];
- la certificazione del personale: assicura che determinate figure professionali possiedano, mantengano e migliorino nel tempo la necessaria competenza, intesa come l'insieme delle conoscenze, delle abilità e delle doti richieste per i compiti assegnati. Ha particolare valore per la corretta realizzazione di attività di particolare criticità, per le quali la sola disponibilità di risorse strumentali e procedure operative può non essere sufficiente.

La credibilità delle certificazioni dipende dalle Organizzazioni che le emettono; la qualificazione degli Organismi di Certificazione viene indicata con il termine "accreditamento".

Si tratta di procedure eseguite da Enti di parte terza (Enti di accreditamento: in Italia ACCREDIA www.accredia.it) che si assumono l'onere di accertare l'oggettiva aderenza da parte degli Organismi di Certificazione alle prescrizioni indicate dalle diverse norme che ne regolano l'attività.

[2] Per un approfondimento mirato sui Sistemi di Gestione conformi a standard tecnici di riferimento, con applicazione singola o integrata e relativo meccanismo di certificazione, si rimanda più diffusamente a P. Baldin, G.R. Stumpo, *Nuovi Strumenti per lo Studio professionale - Norme Uni En ISO 9001:2015, Gestione dei rischi, Sicurezza delle informazioni, Business continuity, Responsabilità sociale, Anticorruzione e altre norme tecniche sui Sistemi di Gestione Integrati,* Collana Prontuari, Bologna, Filodiritto ed. (Aprile 2017).

In Italia, in Europa e nel mondo la serie di norme tecniche ISO/IEC 17000 rappresenta il quadro di riferimento normativo imprescindibile per gli Enti di accreditamento e per gli Organismi di Certificazione (di prodotti/servizi, di Sistemi di Gestione, del personale, di ispezione e per i laboratori di prova e taratura), poiché esplicitano i requisiti di professionalità e di competenza che gli Organismi ed i laboratori devono soddisfare.

Con riferimento all'iter certificativo, nel silenzio sul punto da parte del Regolamento, vale la pena di citare i "passaggi di processo" che portano l'Operatore di mercato a conseguire la certificazione di sistema; tale essendo – tra le tipologie sopra dette – quella per l'Italia maggiormente diffusa nel contesto azienda.

Come funziona quindi il processo di una "certificazione di sistema"?

Una volta che l'Organizzazione abbia scelto su base volontaria lo standard di riferimento e quindi abbia implementato correttamente al proprio interno la metodologia organizzativa suggerita dai requisiti di cui alla specifica norma tecnica di riferimento, ed abbia maturato altresì la decisione di far certificare da Ente terzo accreditato il proprio collegato Sistema Gestionale, essa dovrà prima di tutto procedere alla ricerca dell'Organismo di certificazione che corrisponda alle proprie esigenze ed al ramo di attività che essa sviluppa.

E invero in Italia gli Organismi di certificazione accreditati a livello nazionale sono una cinquantina; ciascuno accreditato per uno o più settori di certificazione relativi ai vari raggruppamenti merceologici di prodotto/servizio.

Sempre sul piano procedurale, individuato l'Organismo di certificazione che fa al caso, l'Organizzazione riceverà il formulario per la domanda di certificazione ed il relativo regolamento.

Nella domanda è importante specificare in maniera chiara ed inequivocabile "il campo di applicazione della certificazione" scelto.

È questo un aspetto molto importante, là ove si consideri che la certificazione ha una propria "spendibilità" sul mercato nazionale – internazionale di riferimento, e quindi bisogna fornire a livello contenutistico e di certificato, un'informazione non ambigua, trasparente e veritiera.

Nella domanda di certificazione l'Organizzazione dovrà anche specificate le sedi da certificare, ove queste siano più di una (e si opti ad es. per certificarne una sola).

Scelto l'Organismo e presentata la domanda, si dovrà poi inviare allo stesso le c.d. "informazioni documentate" sviluppate in conformità ai

requisiti dello standard (di norma minimamente un Manuale, una Politica e delle Procedure) al fine di permettere all'Ente terzo la valutazione della conformità (formale e sostanziale) di esse, rispetto ai requisiti di cui alla norma tecnica di riferimento.

In un momento successivo un *Auditor* inviato dall'Organismo di certificazione verificherà direttamente sul campo, ossia presso l'Operatore di mercato e attraverso il processo di *Audit* (i.e. verifica e controllo), la reale, corretta e completa applicazione della norma tecnica di riferimento all'interno dell'Organizzazione; controllando se quanto "documentato in forma scritta in collegamento allo standard" risulti effettivamente implementato dalle persone operative internamente che realizzano processi, attività e business.

Nel caso in cui l'Organismo rilevi degli "scostamenti" e delle "non conformità" nell'applicazione delle regole formalmente/sostanzialmente conformi allo standard, questi dovranno essere eliminati e corretti. Pena altrimenti il mancato rilascio della "certificazione di conformità".

Diversamente alla fine del processo di verifica e controllo andato a buon fine, l'Organismo emetterà il certificato (valevole per tre anni e rinnovabile nel tempo), sotto forma di una "attestazione" che specifica i settori di certificazione e le sedi certificate.

Il significato della certificazione, nelle sue diverse tipologie, nel relativo iter di processo e nella sua rilevanza in termini di "messaggio di fidatezza" che l'Operatore – per il suo tramite- può dare al Cliente ed agli Stakeholders, al mercato, non è esplicitato dal Regolamento; che pur tuttavia dedica al tema specifiche disposizioni informative ed alcune previsioni programmatiche.

3.1. *Certificazione di sistema ed informazioni esplicative nel Regolamento*

A livello di informativo, e con specifico riferimento al Sistema delle certificazioni, sono esplicitati nel Regolamento i seguenti punti:

i) natura volontaria e trasparente del processo di certificazione (cfr. art. 42 comma 3 del Regolamento: "la certificazione è volontaria e accessibile tramite una procedura trasparente");

ii) soggetti competenti a rilasciare la certificazione e criteri applicativi (cfr. art. 42 comma 5 del Regolamento: "la certificazione ai sensi

del presente articolo è rilasciata dagli Organismi di certificazione di cui all'art. 43 o dall'autorità di controllo competente in base a criteri approvati da tale autorità di controllo competente ai sensi dell'art. 58 par.3, o dal comitato, ai sensi dell'art. 63. Ove i criteri siano approvati dal comitato, ciò può risultare in una certificazione comune, il sigillo europeo per la protezione dei dati");

iii) doveri di collaborazione attiva dell'Operatore di mercato che intende certificarsi con gli Organismi di certificazioni competenti (cfr. art. 43 comma 6 del Regolamento: «il titolare del trattamento o il responsabile del trattamento che sottopone il trattamento effettuato al meccanismo di certificazione fornisce all'Organismo di certificazione di cui all'art. 43 o, ove applicabile all'autorità di controllo competente tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione»);

iv) durata, rinnovabilità e revocabilità della certificazione (cfr. art. 43 comma 7 del Regolamento: «la certificazione è rilasciata al titolare o responsabile del trattamento per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché continuino ad essere soddisfatti i requisiti pertinenti. La certificazione è revocata, se del caso, dagli Organismo di certificazione di cui all'art. 43 o dall'autorità di controllo competente, a seconda dei casi, qualora non siano o non siano più soddisfatti i requisiti della certificazione»).

Il Regolamento contiene anche informazioni che illustrano il "meccanismo di accreditamento" degli Organismi di certificazione; e quindi richiama i requisiti di competenza loro imposti per essere accreditati a livello internazionale, europeo e nazionale; con indicazione anche dei soggetti istituzionalmente deputati alla funzione di controllo delle loro competenze.

L'art. 43 del Regolamento dispone infatti sul punto che:

«1. Fatti salvi i compiti e i poteri dell'Autorità di controllo competente di cui agli artt. 57 e 58, gli Organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati, rilasciano e rinnovano la certificazione, dopo averne informato l'autorità di controllo al fine di consentire alla stessa di esercitare i suoi poteri a norma dell'art. 58, par. 2, lett. h), ove necessario. Gli SM garantiscono che tali Organismi di certificazione siano accreditati da uno o entrambi i seguenti Organismi:

a) Autorità di controllo competente ai sensi degli artt. 55 o 56; (i.e. per l'Italia, il Garante privacy);

b) Organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'Autorità di controllo competente ai sensi degli artt. 55 o 56»[3] (i.e. per l'Italia, Accredia).

Gli Organismi di certificazione accreditati come sopra, sono responsabili della corretta valutazione del processo che comporta il rilascio (o la revoca) della certificazione[4]; fatta salva in ogni caso, per previsione della normativa cogente in esame «la responsabilità del titolare (o del responsabile del trattamento), riguardo alla conformità al Regolamento» (cfr. art. 43 comma 4 del Regolamento).

Nel Regolamento si rinvengono poi previsioni di natura programmatica sulla certificazione.

Previsioni, da cui si evince che, allo stato, mancano di fatto per gli Operatori di mercato interessati al suo rilascio /ottenimento, i presupposti di normazione tecnica atti a mettere in piedi il processo di certificazione.

Sul punto infatti il Regolamento:

a) rimette alla competente Autorità di stabilire i requisiti di accreditamento degli Organismi di certificazione ed al comitato: i) di defini-

[3] Si ricorda che requisiti per l'accreditamento imposti agli Organismi ai sensi dell'art. 43 comma 2 del Regolamento sono: i) dimostrazione all'Autorità competente di indipendenza e competenza riguardo al contenuto della certificazione; ii) impegno nel rispetto dei criteri di cui all'art. 42, par. 5 del Regolamento, come approvati dall'autorità di controllo competente o dal comitato; iii) istituzione a loro cura di procedure per il rilascio, il riesame periodico e il ritiro delle certificazioni, dei sigilli e dei marchi di protezione dei dati; iv) istituzione a loro cura di procedure e strutture atte a gestire i reclami relativi a violazioni della certificazione, rendendole trasparenti per gli interessati ed il pubblico; v) dimostrazione convincente all'Autorità di controllo competente che compiti e funzioni svolti non ingenerano conflitti di interessi. Il comma 3 dello stesso art. 43 ulteriormente aggiunge che: «l'accreditamento degli Organi di certificazione di cui ai par. 1 e 2 del presente articolo ha luogo in base ai criteri approvati dall'Autorità di controllo competente ai sensi degli artt. 55 o 56 o dal comitato, ai sensi dell'art. 63. In caso di accreditamento ai sensi del par. 1, lett. b), del presente articolo, tali requisiti integrano quelli previsti dal regolamento (CE) n. 765/2008 nonché le norme tecniche che definiscono i metodi e le procedure degli Organismi di certificazione». L'accreditamento è rilasciato per un periodo massimo di cinque anni, rinnovabile alle stesse condizioni.

[4] In proposito ex art. 43 comma 5: «L'Organismo di certificazione di cui al par. 1 trasmette all'Autorità di controllo competente i motivi del rilascio o della revoca della certificazione richiesta».

re dei criteri per il rilascio della certificazione (cfr. art. 43 comma 6 del Regolamento: «I requisiti di cui al par. 3 del presente articolo e i criteri di cui all'art. 42, par. 5, sono resi pubblici dall'Autorità di controllo in forma facilmente accessibile. Le Autorità di controllo provvedono a trasmetterli anche al comitato»); ii) di istituire un registro contenente certificazioni e sigilli (cfr. art. art. 42 comma 8 del Regolamento: «il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato»; cfr. art. 43 comma 6 del Regolamento: «Il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato»).

b) rimanda alla Commissione UE la competenza per: i) emanare atti delegati di chiarimento sui requisiti della certificazione dei dati (cfr. art. 43 comma 8 del Regolamento: «Alla Commissione è conferito il potere di adottare atti delegati conformemente all'art. 92 al fine di precisare i requisiti di cui tenere conto per i meccanismi di certificazione della protezione dei dati di cui all'art. 42, par. 1»); ii) adottare atti di esecuzione per stabilire le norme tecniche su certificazione, sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscerli sul mercato (cfr. art. 43 comma 9 del Regolamento: «La Commissione può adottare atti di esecuzione per stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere tali meccanismi di certificazione, i sigilli e marchi di protezione dei dati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'art. 93, par. 2»).

Nelle more dei provvedimenti di cui alle previsioni programmatiche del Regolamento, Accredia ed il Garante privacy nazionale sono intervenuti a chiarimento del sistema delle certificazioni. In particolare, con il comunicato stampa congiunto del 18 Luglio 2017[5] le suddette Autorità istituzionali hanno richiamato l'attenzione degli Operatori di mercato sulla necessità – dell'allineamento agli obblighi di adeguamento al Regolamento con particolare in attinenza alle misure tecniche ed organizzative, suggerendo però di attendere la definizione di requisiti comuni per la conformità delle certificazioni, e sottolineando come vi siano col-

[5] Cfr. Comunicato stampa del Garante privacy – Accredia pubblicato nel sito del Garante www.garanteprivacy.it, "Regolamento UE e certificazione in materia di dati personali".

laborazioni in corso, al fine di cercare di rispettare la scadenza di diretta applicabilità, del 25 Maggio 2018 per interventi sul punto.

Entrambi i soggetti istituzionali coinvolti, come da comunicato sopra citato, rimarcano in particolare che «… al momento le certificazioni di persone, nonché quelle emesse in materia di privacy o data protection eventualmente rilasciate in Italia, sebbene possano costituire una garanzia e atto di diligenza verso le Parti Interessate dell'adozione volontaria di un sistema di analisi e controllo dei principi e delle norme di riferimento, a legislazione vigente non possono definirsi conformi agli artt. 42 e 43 del Regolamento n. 679/2016/UE, poiché devono ancora essere determinati i "requisiti aggiuntivi", ai fini dell'accreditamento degli Organismi di certificazione ed i criteri specifici di certificazione».

4. *La certificazione delle competenze: il disposto del Regolamento e la norma tecnica UNI 11007*

Il tema della certificazione preso in considerazione dal Regolamento, non si esaurisce a quanto sopra, ma rileva anche sotto diverso profilo in relazione all'adempimento imposto al titolare di costruire un "Organigramma privacy" che possa supportarlo nella realizzazione degli adempimenti operativi imposti, con ricorso a persone competenti e capaci.

Sul punto il Regolamento richiede al titolare di procedere con atti di designazione, nomina ed istruzione, previa valutazione delle effettive competenze dei soggetti scelti; in modo da poter fornire anche "garanzie sufficienti" a comprovare la capacità di responsabili (ed addetti) al trattamento, ad assolvere gli adempimenti operativi per suo conto, sia in conformità delle regole imposte dallo stesso Regolamento, sia a garanzia della tutela dei diritti degli interessati.

Il tema della "qualifica delle competenze" – e relativa certificazione, si pone quindi in tutta evidenza, per le scelte di designazione e nomina che il Regolamento pone in capo al titolare.

E ciò, in particolare, per quanto attiene:

i) alla figura del responsabile del trattamento (da designarsi con i compiti di cui a specifico contratto da formalizzare *ad hoc ex* art. 28 comma 3 del Regolamento), posto che in proposito si dispone che: «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 ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garanzia della tutela dei diritti dell'interessato» (cfr. Capo IV art. 28 comma 1 del Regolamento) e,

ii) alla figura del responsabile della protezione dei dati DPO - *Data Protection Officer* (da scegliersi tra un dipendente o un soggetto esterno in base a specifico contratto di servizi, sussistendo i presupposti per la designazione di cui all'art. 37 e per i compiti di cui all'art. 39 del Regolamento), dato che sempre la norma europea prescrive di scegliere la figura nel ruolo: «in funzione delle qualità professionali ed in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità» – operativa –, «di assolvere» – minimamente (cfr. art. 38 comma 6 del Regolamento) «i compiti di cui all'art. 39» (i.e. informativa e consulenza in merito agli obblighi del Regolamento; sorveglianza dell'osservanza del Regolamento, della privacy policy, del quadro delle responsabilità ed autorità allocate e dei doveri di sensibilizzazione e formazione del personale che partecipa ai trattamenti; pareri – su richiesta – in merito alla valutazione d'impatto, sorvegliandone lo svolgimento; cooperazione con l'Autorità di controllo; fungere da punto di contatto per la predetta Autorità e per gli interessati dal trattamento).

Con obbligo di correlata presa in considerazione da parte sempre del titolare, per la figura da inserire in Organigramma nel ruolo di DPO, anche della sua capacità valutativa dei rischi inerenti alle attività di trattamento «tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo» (cfr. art. 39 comma 2 del Regolamento).

Come può il titolare esercitare positivamente l'onere della prova, di aver effettuato una "scelta adeguata" e *compliant* con i requisiti del Regolamento, in relazione alla corretta scelta, nella designazione delle due figure principali di cui all'Organigramma privacy?

Sul punto, rileva la "presunzione di conformità", documentabile con il rilascio di certificazione. In proposito infatti:

- quanto al responsabile del trattamento- ai sensi e per gli effetti dell'art. 28 comma 5 del Regolamento: "l'adesione da parte del Responsabile del trattamento ad un codice di condotta approvato di cui all'art. 40 o a un meccanismo di certificazione approvato di cui all'art. 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai par. 1 e 4 del presente articolo";

- quanto al responsabile della protezione dei dati (DPO) – i requisiti di conoscenza, competenza e capacità non specificati direttamente dal Regolamento, sono regolamentati nelle Linee Guida[6] sui Responsabili della protezione dei dati del Gruppo di lavoro art. 29 per la protezione dei dati n. 16/IT – WP243 rev. 01.

A livello di normazione tecnica, va detto che esiste peraltro già la norma nazionale UNI 11697 (Attività professionali non regolamentate Profili professionali relativi al trattamento ed alla protezione dei dati personali)[7] che:

i) «definisce i principali profili professionali nell'ambito del trattamento della protezione dei dati personali al fine di stabilire requisiti fondamentali per l'insieme di conoscenze abilità e competenze che le contraddistinguono» (cfr. introduzione della norma tecnica UNI);

ii) declina in modo specifico i requisiti di qualificazione, conoscenza, abilità e competenza delle seguenti nuove figure professionali: Responsabile della protezione dei dati – DPO; *Manager Privacy*; Verificatore Privacy; *Specialist Privacy*.

La norma tecnica UNI precisa che, per qualificarsi nei ruoli di cui sopra, occorre che compiti ed attività inerenti alla professione vengano descritti «sulla base delle funzioni effettivamente svolte dai professionisti operanti nell'ambito del trattamento e della protezione dei dati personali nei differenti contesti lavorativi; si tratta di funzioni molteplici e che riguardano aspetti tecnici, amministrativi, culturali, scientifici, legali» (cfr. Scopo e campo di applicazione della norma tecnica UNI).

Allo stato, si attende la conversione della predetta norma nazionale UNI 11697 a norma europea CEN.

4.1. *I requisiti di qualificazione tecnica della figura del DPO* (Data Protection Officer)

Senza entrare nel merito dell'intero articolato dello standard tecnico UNI sopra detto, può tuttavia risultare interessante – oltreché significa-

[6] Le Linee guida sono reperibili nel sito del Garante privacy www.garanteprivacy.it. .

[7] La norma tecnica UNI 11697, così come tutte le altre diverse norme UNI citate nel testo sono acquistabili presso UNI – Ente Nazionale Italiano di Unificazione (www.uni.com).

tivo – prendere visione dei requisiti di formazione ed addestramento che portano il professionista a potersi qualificare nel ruolo di DPO, come da percorso mirato previsto dalla predetta norma tecnica ISO di riferimento, già operativa e disponibile sul mercato.

Quali sono i requisiti richiesti al DPO dagli standard tecnici internazionali? (estratto dalla norma UNI 11697):

«Profilo professionale del Responsabile della protezione dei dati (*Data Protection Officer*):

Definizione sintetica: Supporta titolare o responsabile dell'applicazione del Regolamento UE 2016/679;

Missione: fornisce al titolare/ responsabile del trattamento il supporto indispensabile ad assicurare l'osservanza del Regolamento UE 2016/679;

Risultati attesi (*Deliverables*):

a) Responsabile (*Accountable*)

- relazioni periodiche sull'osservanza delle norme di legge in materia di protezione dei dati personali;
- documentazione a supporto della richiesta di consultazione preventiva all'Autorità di controllo a seguito di valutazione di impatto ex Regolamento UE 2016/679;
- richiesta di consultazione alle Autorità di controllo su questioni applicative specifiche;
- documentazione relativa alle attività di interfacciamento con l'Autorità di controllo (richieste di informazione, procedure di accertamento verifica, notifica di eventuali violazioni di dati personali);
- documentazione (inclusa modulistica) di interfaccia con gli interessati;
- indicatori sulla protezione dei dati personali.

b) Referente (*Responsabile*): programma di formazione, aggiornamento e consapevolezza; pareri su valutazione di impatto *ex* Regolamento UE /2016/679;

c) Collaboratore (*Contributor*): attribuzione delle responsabilità in ambito trattamento e protezione dei dati personali; budget per la protezione dei dati personali; politica della protezione dei dati personali; requisiti per il trattamento e la protezione dei dati personali; procedure operative per trattamento e protezione dei dati personali; valutazione di impatto sulla protezione dei dati; valutazione del rischio relativo alla sicurezza

delle informazioni; piano di trattamento del rischio relativo alla sicurezza delle informazioni; codici di condotta; programma di audit per la protezione ed il trattamento dei dati personali.

Compiti principali: informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento il merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli SM relative alla protezione dei dati, nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati, e sorvegliarne lo svolgimento; cooperare con l'Autorità di controllo; fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento.

COMPETENZE e- CF ASSEGNATE (E- CF 3.0)	**Livello**
A.4. Pianificazione di prodotto/ di servizio	3
D.1 Sviluppo della strategia per la sicurezza informatica	4
D.8 Gestione del contratto	3
D.9 Sviluppo del personale	3
E.3 Gestione del rischio	4
E.4 Gestione delle relazioni	4
E.8 Gestione della sicurezza dell'informazione	3
E.9 Governance dei sistemi informativi	4

Abilità (*Skills*): contribuire alla strategia per il trattamento e per la protezione dei dati personali; gestire l'applicazione dei codici di condotta e delle certificazioni applicabili in materia di trattamento e protezione dei dati; capacità di comunicare; capacità di analisi; autogestione e controllo dello stress; capacità di autosviluppo; capacità di controllo; capacità di convincimento; capacità di gestione dei conflitti; iniziativa; idoneità alla negoziazione; capacità organizzative; pensiero prospettico; pianificazione programmazione; atteggiamento costruttivo nella soluzione dei problemi; tenacia;

S1 – affrontare le esigenze della formazione continua del personale per soddisfare le esigenze dell'Organizzazione;
S5 – analizzare gli asset critici dell'azienda ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi;
S19 – anticipare i cambiamenti richiesti alla strategia aziendale dell'*information security* e formulare nuovi piani;
S21 – applicare azioni di contenimento del rischio e dell'emergenza;
S23 – applicare gli standard, le *best practice* e i requisiti legali più rilevante all'*information security*;
S40 – *coaching*;
S52 – comunicare e pubblicizzare sia risultati dell'analisi del rischio che i processi di gestione del rischio;
S55 – comunicare le buone e cattive notizie per evitare sorprese;
S66 – costruire un piano di gestione del rischio e fornire e produrre piani di azione preventivi;
S91 – garantire che la proprietà intellettuale e le norme della privacy siano rispettate;
S111- identificare *gap* di competenze e *skill gaps*;
S140 – negoziare termini e condizioni del contratto;
S153 – preparare i *template* per pubblicazioni condivise;
S156 – progettare e documentare i processi dell'analisi e della gestione del rischio;
S167 – raccogliere la conoscenza interna ed esterna e i fabbisogni di informazione;
S171 – rendere l'informazione disponibile;
S172 – rispondere all'esigenza di sviluppo professionale del personale per soddisfare le esigenze organizzative;
S176 – seguire/controllare l'uso effettivo degli standard documentativi aziendali;
S187 – sviluppare piani di *risk management* per identificare le necessarie azioni preventive.

Conoscenze (*Knowledge*): i principi di privacy e protezione dei dati by design e by default; i diritti degli interessati previsti da leggi e regolamenti vigenti; le responsabilità connesse al trattamento dei dati personali; norme di legge italiane ed europee in materia di trattamento e di protezione dei dati personali; norme di trasferimento dei dati personali all'e-

stero e circolazione dei dati personali extra UE/SEE; le metodologie di valutazione di impatto sulla protezione dei dati e PIA - Privacy Impact Assessment; le possibili minacce alla protezione dei dati personali; le norme tecniche ISO/IEC per la gestione dei dati personali; i codici di condotta e le certificazioni applicabili in materia di trattamento e protezione dei dati personali; tecniche e strumenti di comunicazione (relazioni con Istituzioni, Autorità, Forze dell'ordine, enti locali e stampa); le tecniche crittografiche; le tecniche di anonimizzazione; le tecniche di pseudonimizzazione; sistemi e tecniche di monitoraggio e "reporting";

K26 – gli strumenti di controllo della versione per la produzione di documentazione;

K49 – i metodi di sviluppo delle competenze;

K60 – i processi dell'organizzazione ivi inclusi le strutture decisionali, di budget e di gestione;

K67 – i rischi critici per la gestione della sicurezza;

K71 – i tipici KPI (*Key Performance Indicators*);

K83 – il potenziale e le opportunità offerte dagli standard e dalle best practice più rilevanti;

K85 – il ritorno dell'investimento comparato l'annullamento del rischio;

K98 – l'impatto dei requisiti legali sulla sicurezza dell'informazione;

K108 – la computer forensics (analisi criminologica di sistemi informativi);

K115 – la politica di gestione della sicurezza nelle aziende e delle sue implicazioni con gli impegni verso i clienti, i fornitori, e sub-contraenti;

K122 – la strategia dell'informazione nell'Organizzazione;

K130 – le best practice (metodologiche) e gli standard nell'analisi del rischio;

K132 – le best practice e gli standard nella gestione della sicurezza delle informazioni;

K139 – le metodologie di analisi dei fabbisogni di competenze e *skill*;

K149 – le norme legali applicabili contratti;

K152 – le nuove tecnologie emergenti (per es. sistemi distribuiti, modelli di virtualizzazione, sistemi di mobilità, data sets)».

Luci ed ombre del regime delle diverse tipologie di certificazione previste dal GDPR – General Data Protection Regulation

Al fine di migliorare la trasparenza ed il rispetto delle regole sulla tutela del dato, il Regolamento UE 697/2016 vincolante per il 28 SM dal 25 maggio 2018 incoraggiata l'istituzione di meccanismi di certificazione, sigilli e marchi di protezione che consentano agli interessati di valutare rapidamente il livello di protezione dei dati oggetto di trattamento. Tali sistemi, che richiamano gli standard tecnici ed internazionali ISO, rilevano a favore del titolare, nel fornire la prova di aver adottato "misure tecniche ed organizzative adeguate" al contenimento ed alla gestione dei rischi collegati ad ogni trattamento ed anche di essersi dotato di un "organigramma privacy" – con figure di ruolo adeguatamente formate, competenti e capaci, rispetto ai compiti ed agli adempimenti imposti dallo stesso Regolamento.

Standards ISO and different certification mechanisms according to the Regulation UE 697/2016

To enhance transparency and compliance with the rules on personal data protection the Regulation UE 697/2016, in force and binding the 28 European Member States since May 25, encourages the establishment of certification mechanisms, data protection seals and marks, in order to allow data subjects to quickly assess the level of protection relating to data processings.
Certification mechanisms, based on international and technical standards ISO, play an important role in the scope of the Regolation, as they support the Data Controller in the evidence of appropriate technical and organisational measures prescripted, to ensure and to demonstrate that processings are performed in accordance with the rules established, and also that data processors and people authorised to process in the organization, are fully and correctly trained, prepared and competent to operate in compliance with the Regulation.

Ciberspazio e Diritto vol. 19, n. 60 (1-2 - 2018), in questo numero:

isbn 978-88-7000-792-3

9 788870 007923

autorizzazione del Tribunale di Modena, n. 1507 del 10/12/1999 - prezzo del presente numero € 30,00 i.c.