Le certificazioni nel nuovo regolamento UE sulla privacy

Cybersecurity e Data Protection

Università di Bologna

11 May 2017

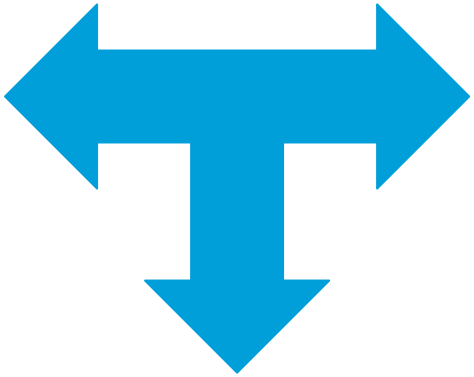
DNV GL

- Con l'obiettivo di **salvaguardare la vita, la proprietà e l'ambiente**, DNV GL consente alle organizzazioni di incrementare la sicurezza e la sostenibilità delle proprie attività.
- DNV GL fornisce servizi di certificazione in tutti i settori merceologici, di classificazione o verifica per i settori maritime, oil & gas e energy.
- Opera in oltre 100 Paesi con 15.000 professionisti impegnati ad aiutare i propri clienti a rendere **il mondo più sicuro, più intelligente e più verde**.
- Investiamo il **5%** dei nostri ricavi annuali in ricerca ed innovazione

Le “certificazioni”

Fra le novità previste dal GDPR (EU General Data Protection Regulation) per poter dimostrare la propria conformità alla normativa vi sono i **codici di condotta** e le **certificazioni**. Si tratta di meccanismi ai quale i Titolari e i responsabili possono aderire volontariamente.

Certificazione del SG



Codice di condotta

Certificazione del DPO

La certificazione del SG

Articolo 42

Certificazione

1. Gli Stati membri, le autorità di controllo, il commitato e la Commissine incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonchè di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese.

...

3. la certificazione è volontaria e accessibile tramite una procedura trasparente.

4. La certificazione ai sensi del presente articolo non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti a norma degli articoli 55 e 56.

...

7. La certificazione è rilasciata al titolare del trattamento o responsabile del trattamento per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purchè continuino a essere soddisfatti i requisiti pertinenti. La certificazione è revocata, se del caso, dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente, a seconda dei casi, qualora non siano o non siano più soddisfatti i requisiti per la certificazione.

Quindi la certificazione...

- È **volontaria.**
- Aiuta a dimostrare la propria conformità al GDPR, ma non riduce la responsabilità. di titolari e responsabili, **non è esimente.**
- Ha una durata massima di **3 anni**, dopo di che deve essere rinnovata.
- Può essere **revocata**.

Ma chi la può rilasciare?

Articolo 42

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

Quindi le certificazioni possono essere rilasciate da diversi organismi:

- il **Comitato** (Comitato europeo per la protezione dei dati)
- l'Autorità di Controllo Competente (**Garante per la protezione dei dati personali**)
- Gli **Organismi di Certificazione**

Il filo rosso dei soggetti e delle loro competenze 1/2

COMITATO EUROPEO:

- approva i criteri di accreditamento (art. 43, c 3)
- definisce i criteri di certificazione (art. 42, c 5)
- rilascia certificazioni (art. 42, c 5)
- accredita gli Organismi di certificazione (art. 70, c 1, p o)

AUTORITÀ DI CONTROLLO competente (Garante):

- approva i criteri di accreditamento (art. 43, c 3)
- definisce i criteri di certificazione (art. 42, c 5, art. 58, c 3, p f)
- rilascia certificazioni (art. 42, c 5)
- accredita gli Organismi di certificazione (art. 43, c 1)

Il filo rosso dei soggetti e delle loro competenze 2/2

ORGANISMO NAZIONALE DI ACCREDITAMENTO:

- accredita gli Organismi di certificazione, basandosi sui criteri di accreditamento (art. 43, c 1)

ORGANISMO DI CERTIFICAZIONE accreditato dall'Autorità di controllo o dal Comitato o dall'Organismo nazionale di accreditamento:

- rilascia certificazioni (art. 42, c 5, art. 43, c1)

La situazione ad oggi

- Al momento il **Comitato**:
  - non ha rilasciato criteri per l'accreditamento
  - non ha rilasciato criteri per la certificazione

- Al momento il **l'Autorità di Controllo (Garante)**:
  - non ha rilasciato criteri per l'accreditamento
  - non ha rilasciato criteri per la certificazione

All'apparenza, quindi, **non sembrerebbe ancora possibile emettere certificazioni** del SG relative al GDPR.

In realtà …

Codice di condotta

Articolo 40

Codici di condotta

1.Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

2.Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento, ad esempio relativamente a:

a) il trattamento corretto e trasparente dei dati;
b) b) i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;
c) c) la raccolta dei dati personali;
d) la pseudonimizzazione dei dati personali;
e) l'informazione fornita al pubblico e agli interessati;
f) l'esercizio dei diritti degli interessati;
g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;
h) le misure e le procedure di cui agli articoli 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32;
i) la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato;
j) il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali;
k) le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli articoli 77 e 79.

Pubblicazione del Codice di Condotta

- I Codici di Condotta elaborati dalle Associazioni o dagli Organismi di cui all'Art. 40, c2, **sono sottoposti all'Autorità di controllo competente**.
- Qualora il progetto di codice, la modifica o la proroga siano approvati ai sensi dell'articolo 55, e **se il codice di condotta in questione non si riferisce alle attività di trattamento in vari Stati membri, l'autorità di controllo registra e pubblica il codice.**
- **Qualora il progetto di codice di condotta si riferisca alle attività di trattamento in vari Stati membri**, prima di approvare il progetto, la modifica o la proroga, **l'autorità di controllo** che è competente ai sensi dell'articolo 55 lo sottopone, tramite la procedura di cui all'articolo 63, al **comitato**, il quale formula un parere sulla conformità al regolamento del progetto di codice. Qualora il parere confermi che il progetto di codice di condotta è conforme al regolamento, il comitato trasmette il suo parere alla **Commissione**. La Commissione può decidere che il codice di condotta sottoposto ha validità generale all'interno dell'Unione. La Commissione provvede a dare un'adeguata pubblicità dei codici approvati per i quali è stata decisa la validità generale. Il comitato raccoglie in un registro tutti i codici di condotta approvati e li rende pubblici mediante mezzi appropriati.

Certificazione del Codice di Condotta

Articolo 41

Monitoraggio dei codici di condotta approvati

1. Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 57 e 58, il controllo della conformità con un codice di condotta ai sensi dell'articolo 40 può essere effettuato da un **organismo in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento** a tal fine dell'autorità di controllo competente.

2. L'organismo di cui al paragrafo 1 può essere accreditato a monitorare l'osservanza di un codice di condotta se esso ha [...]

3. [...]

4. Fatti salvi i compiti e i poteri dell'autorità di controllo competente e le disposizioni del capo VIII, un organismo di cui al paragrafo 1 del presente articolo adotta, stanti garanzie appropriate, le opportune misure in caso di violazione del codice da parte di un titolare del trattamento o responsabile del trattamento, tra cui la sospensione o l'esclusione dal codice del titolare del trattamento o del responsabile del trattamento. Esso informa l'autorità di controllo competente di tali misure e dei motivi della loro adozione.

5. L'autorità di controllo competente revoca l'accreditamento dell'organismo di cui al paragrafo 1, se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate dall'organismo violano il presente regolamento.

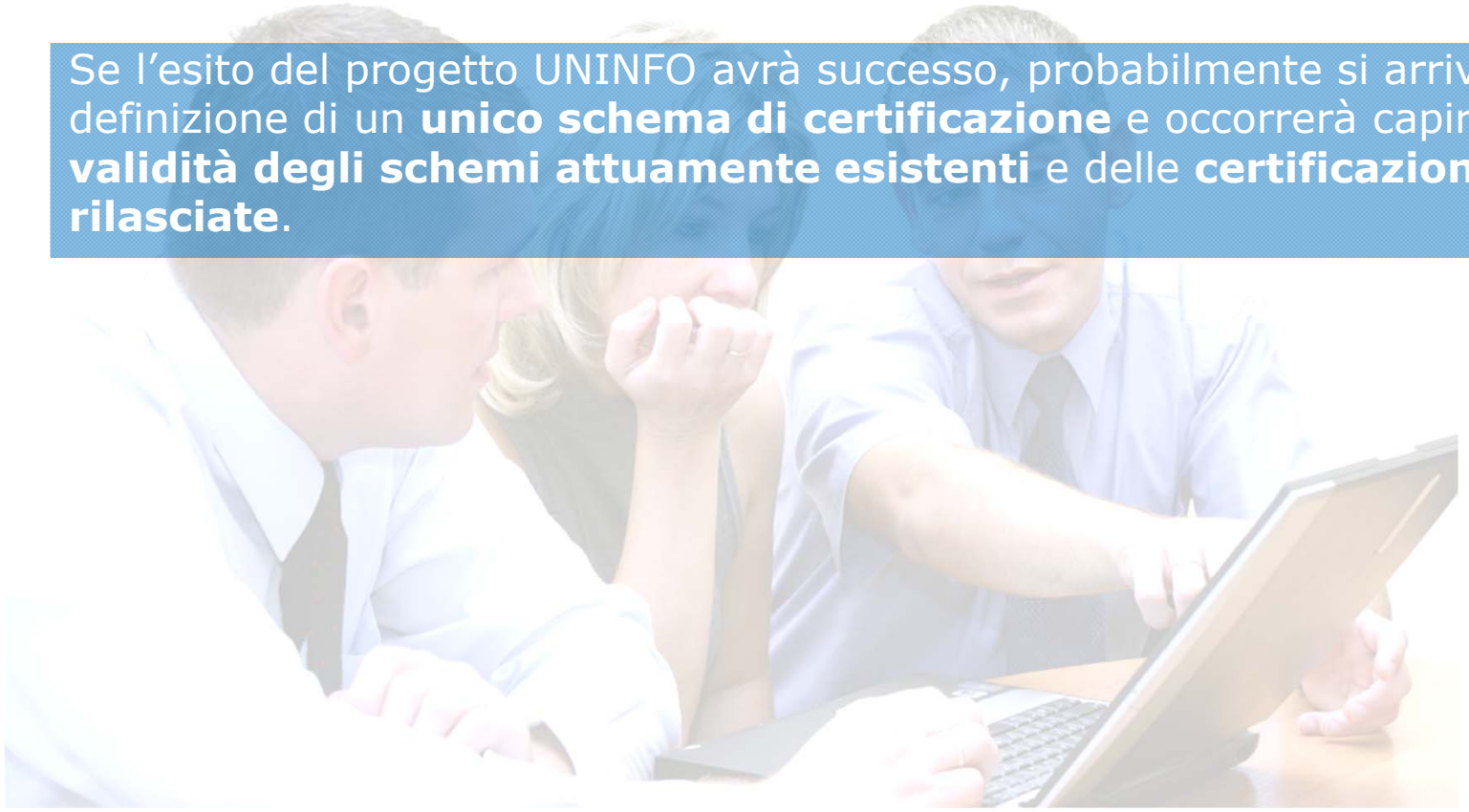
Il Data Protection Officer

- La Sezione 4 del GDPR tratta diffusamente del **DPO**, definendone ruoli, caratteristiche e responsabilità.
- Dovrebbe essere in dirittura finale lo schema per la certificazione unificata per la professione dei **Data Protection Officer (DPO)**, dopo oltre un anno di lavori del tavolo degli esperti UNI INFO.
- La consultazione pubblica sul progetto di norma tecnica UNI/UNINFO "Attività professionali non regolamentate – Profili professionali relativi al trattamento e alla protezione dei dati personali – Requisiti di conoscenza abilità e competenza" (codice progetto E14D00036), che definisce i profili e le competenze dei professionisti che lavorano nel contesto del trattamento e della protezione dei dati personali è scaduta il 25 marzo 2017 e nelle prossime settimane si presume che verrà stabilizzato l'embrione condiviso della norma.

Prospettive della certificazione DPO

- A oggi esistono vari schemi di certificazione delle competenze personali nell'ambito della Data Protection.

Se l'esito del progetto UNINFO avrà successo, probabilmente si arriverà alla definizione di un **unico schema di certificazione** e occorrerà capire **la validità degli schemi attuamente esistenti** e delle **certificazioni già rilasciate**.



@DNVGLBA_IT

DNV GL – Business Assurance Italia

www.dnvgl.com

SAFER, SMARTER, GREENER