I profili professionali privacy alla luce della nuova norma UNI 11697

D. (Mimmo) Squillace

I profili professionali privacy alla luce della nuova norma UNI 11697

D. (Mimmo) Squillace
presidenza@uninfo.it
mimmo_squillace@it.ibm.com

Mimmo Squillace

Technical Relations Executive – IBM Italia

Presidente UNINFO

Agenda

- Norme tecniche
  - Cosa sono, chi le sviluppa, benefici
- UNI ed UNINFO
- APNR/ICT
  - UNI EN 16234
  - UNI 11697
- Certificazione UNI 11697?

Agenda

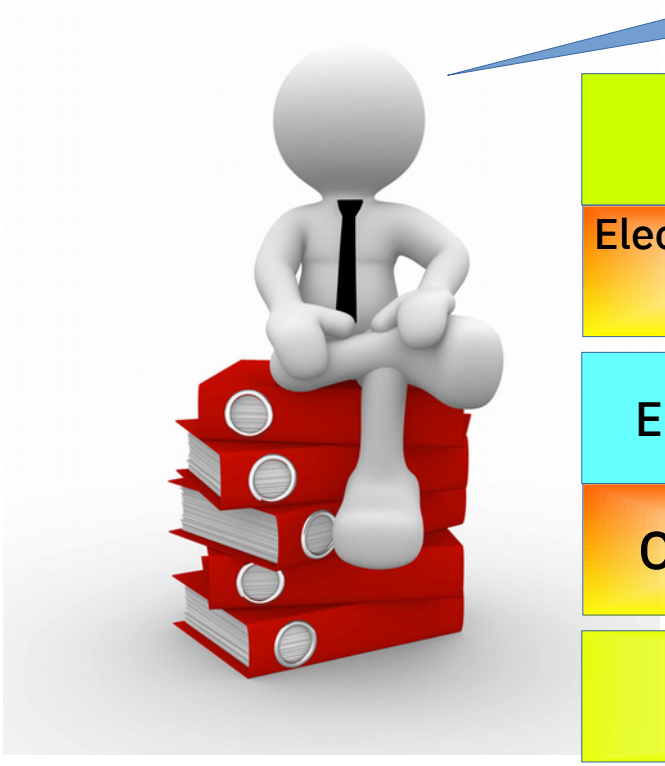
- Norme tecniche
  - Cosa sono, chi le sviluppa, benefici
- UNI ed UNINFO
- APNR/ICT
  - UNI EN 16234
  - UNI 11697
- Certificazione UNI 11697?

Una Norma Tecnica descrive lo “stato dell’arte” di: un bene, un servizio, un processo o, anche, un profilo professionale

La Norma Tecnica è un documento!

*Sviluppato presso un Ente di Normazione in maniera **trasparente** e **democratica,** approvato in maniera **consensuale** ed adottato su **base volontaria.***

Le Norme Tecniche sono sviluppate da:



International Standard Setting Organizations

Electrotechnical	"All-others"	Telecommunication
IEC JTC/1	ISO	ITU

European Standard Setting Organizations

CENELEC	CEN	ETSI

National Standard Bodies

W3C

IETF & IEEE

Fora Consorzi

Promuovono l'interoperabilità
Migliorano Sicurezza prodotti
Consentono Economie di Scala

1 Norma EN:

- equivale a 33 Norme Nazionali
- consente l'accesso ad un mercato di 650 milioni di persone

Agenda

- Norme tecniche
  - Cosa sono, chi li sviluppa, benefici
- **UNI ed UNINFO**
- APNR/ICT
  - UNI EN 16234
  - UNI 11697
- Certificazione UNI 11697?

I National Standards Body italiani sono:

CEI ed UNI

COMITATO ELETTROTECNICO ITALIANO

Sistema UNI
UNINFO => IT

CTI
Termotecnica

CIG
Gas

CUNA
Automobili

UNICHIM
Chimica

UNSIDER
Ferro e Metalli

UNINFO
Informatica

UNIPLAST
Materie Plastiche

I settori di attività di UNINFO

automazione
systems
document
industriale
intelligent
del
software
data
attività
elettronica
firma-elettronica
professionali
MPEG
ID
transportation
fatturazione
ingegneria
digitali
eLearning
eHealth
eBusiness
quality
formats
biometria

Informatica Medica

Ingegneria del SW

Blockchain

eBSF

“MPEG”

Industria 4.0

“Traffico”

Sicurezza informatica

Tecnologie Additive

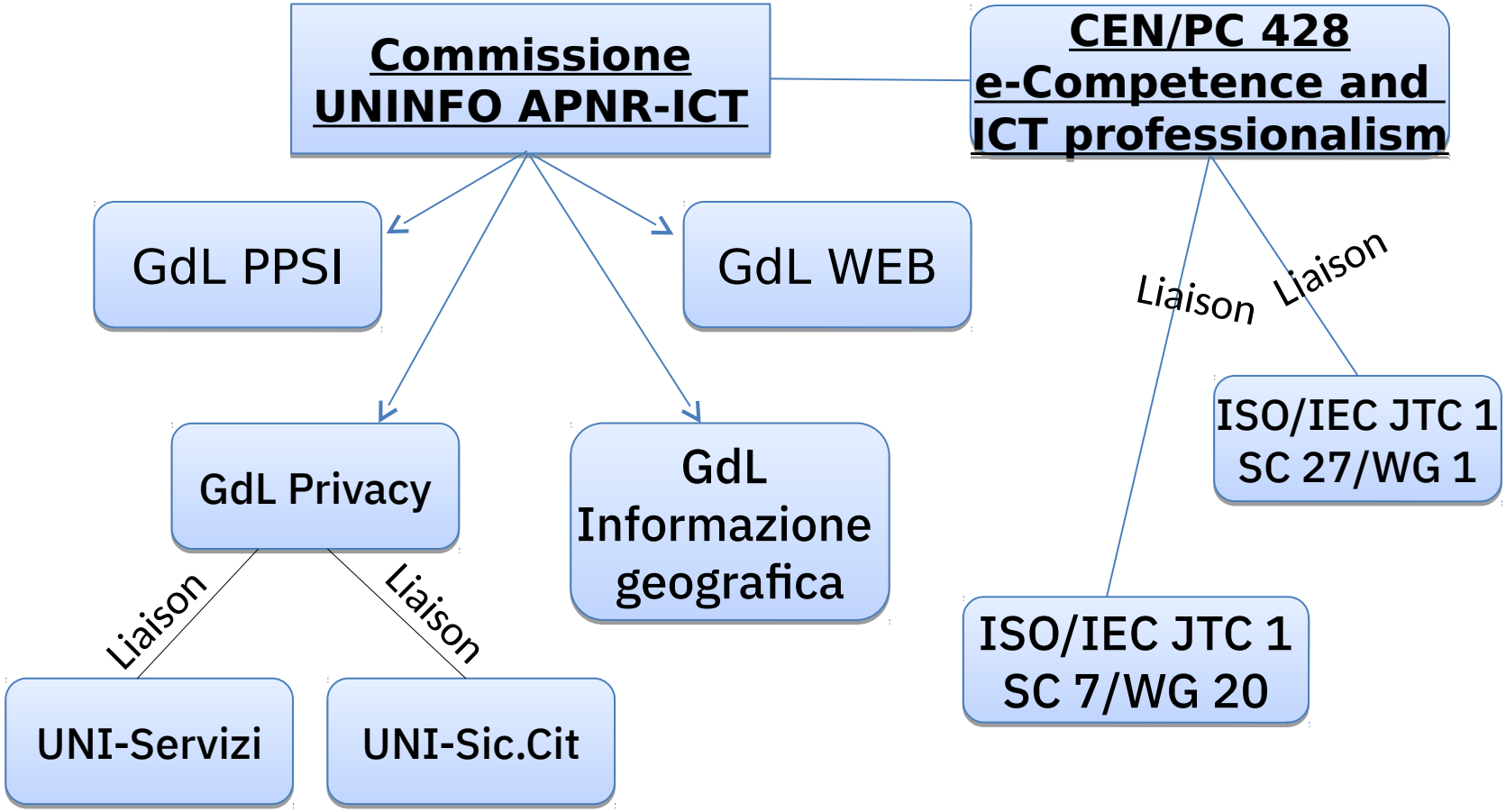
Automazione Ind.

APNR-ICT

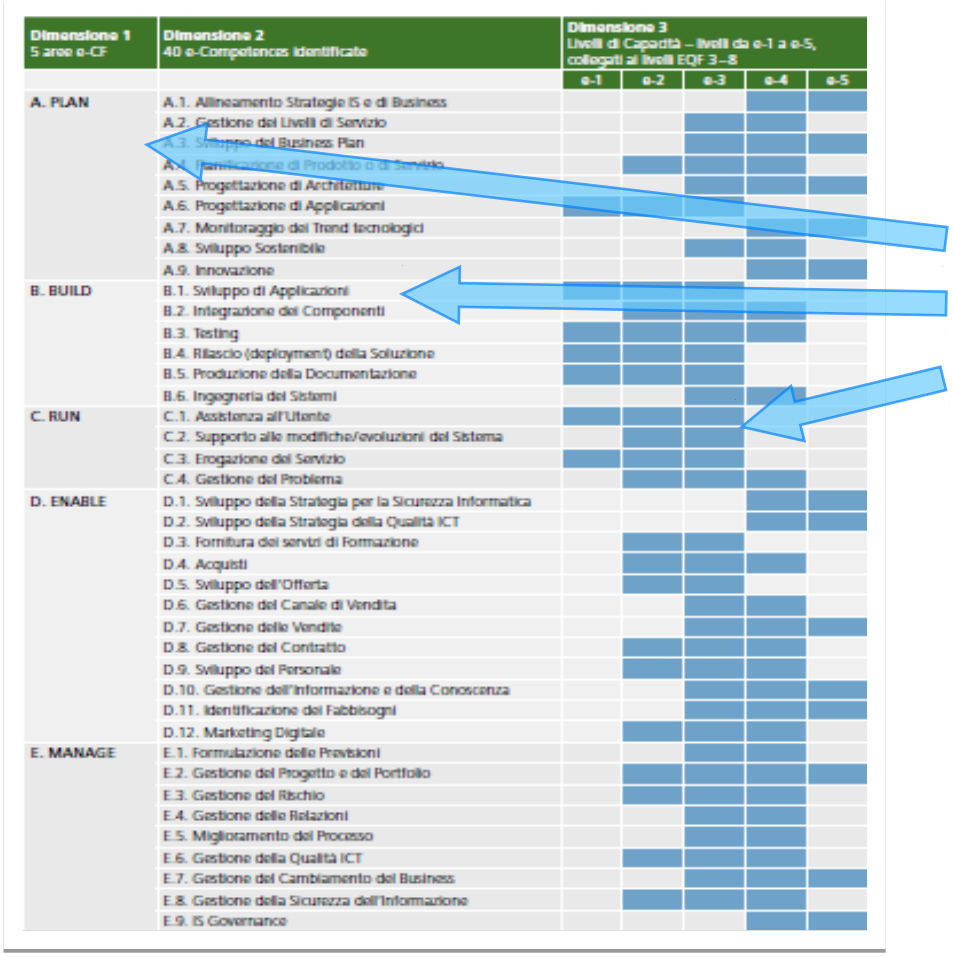
Agenda

- Norme tecniche
  - Cosa sono, chi le sviluppa, benefici
- UNI ed UNINFO
- APNR/ICT
  - UNI EN 16234
  - UNI 11697
- Certificazione UNI 11697?

Attività Professionali Non Regolamentate – ICT



e-CF 3.0 (2014) - EN 16234-1 (2016)



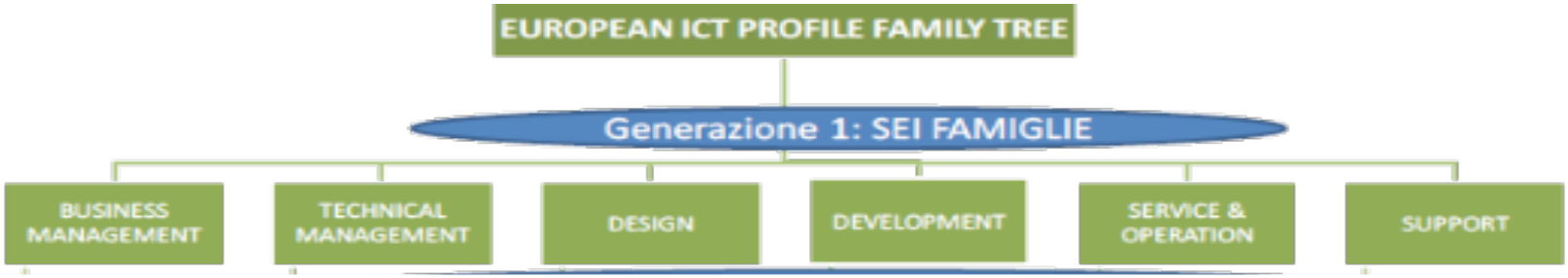
Dimensione 1 5 aree e-CF	Dimensione 2 40 e-Competences identificate	Dimensione 3 Livelli di Capacità – livelli da e-1 a e-5, collegati ai livelli EQF 3–8				
		e-1	e-2	e-3	e-4	e-5
A. PLAN	A.1. Allineamento Strategie IS e di Business					
	A.2. Gestione dei Livelli di Servizio					
	A.3. Sviluppo del Business Plan					
	A.4. Pianificazione di Prodotto o di Servizio					
	A.5. Progettazione di Architetture					
	A.6. Progettazione di Applicazioni					
	A.7. Monitoraggio dei Trend tecnologici					
	A.8. Sviluppo Sostenibile					
	A.9. Innovazione					
B. BUILD	B.1. Sviluppo di Applicazioni					
	B.2. Integrazione dei Componenti					
	B.3. Testing					
	B.4. Rilascio (deployment) della Soluzione					
	B.5. Produzione della Documentazione					
	B.6. Ingegneria dei Sistemi					
C. RUN	C.1. Assistenza all'Utente					
	C.2. Supporto alle modifiche/evoluzioni del Sistema					
	C.3. Erogazione del Servizio					
	C.4. Gestione del Problema					
D. ENABLE	D.1. Sviluppo della Strategia per la Sicurezza Informatica					
	D.2. Sviluppo della Strategia della Qualità ICT					
	D.3. Fornitura dei servizi di Formazione					
	D.4. Acquisti					
	D.5. Sviluppo dell'Offerta					
	D.6. Gestione del Canale di Vendita					
	D.7. Gestione delle Vendite					
	D.8. Gestione del Contratto					
	D.9. Sviluppo del Personale					
	D.10. Gestione dell'Informazione e della Conoscenza					
	D.11. Identificazione dei Fabbisogni					
	D.12. Marketing Digitale					
E. MANAGE	E.1. Formulazione delle Previsioni					
	E.2. Gestione del Progetto e del Portfolio					
	E.3. Gestione del Rischio					
	E.4. Gestione delle Relazioni					
	E.5. Miglioramento del Processo					
	E.6. Gestione della Qualità ICT					
	E.7. Gestione del Cambiamento del Business					
	E.8. Gestione della Sicurezza dell'Informazione					
	E.9. IS Governance					

3 Dimensioni comuni
D1: 5 aree
D2: 40 e-competences
D3: 5 livelli di competenza

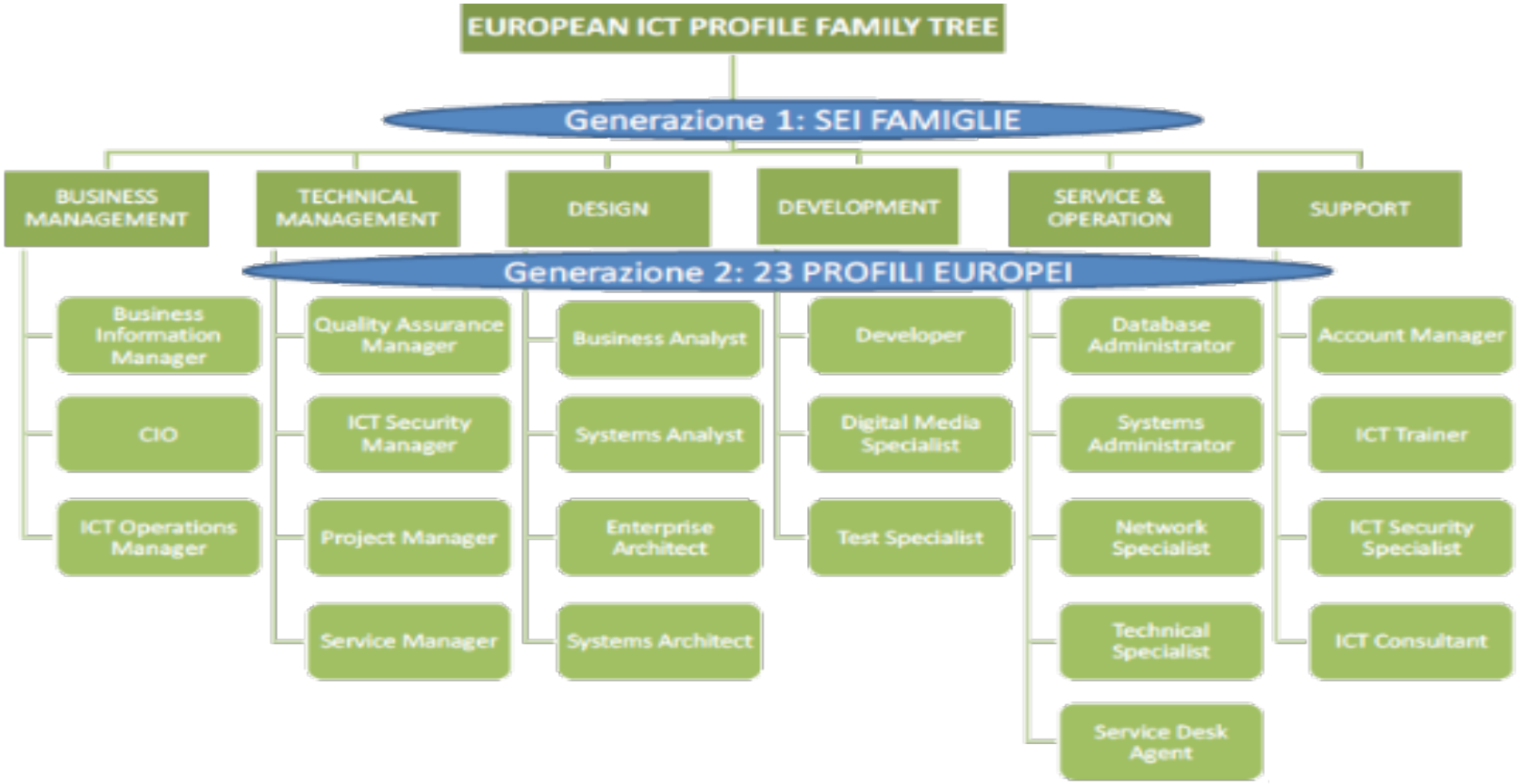
Eventuali profili personalizzati possono sfruttare la quarta dimensione prevista dal modello

http://www.ecompetences.eu/

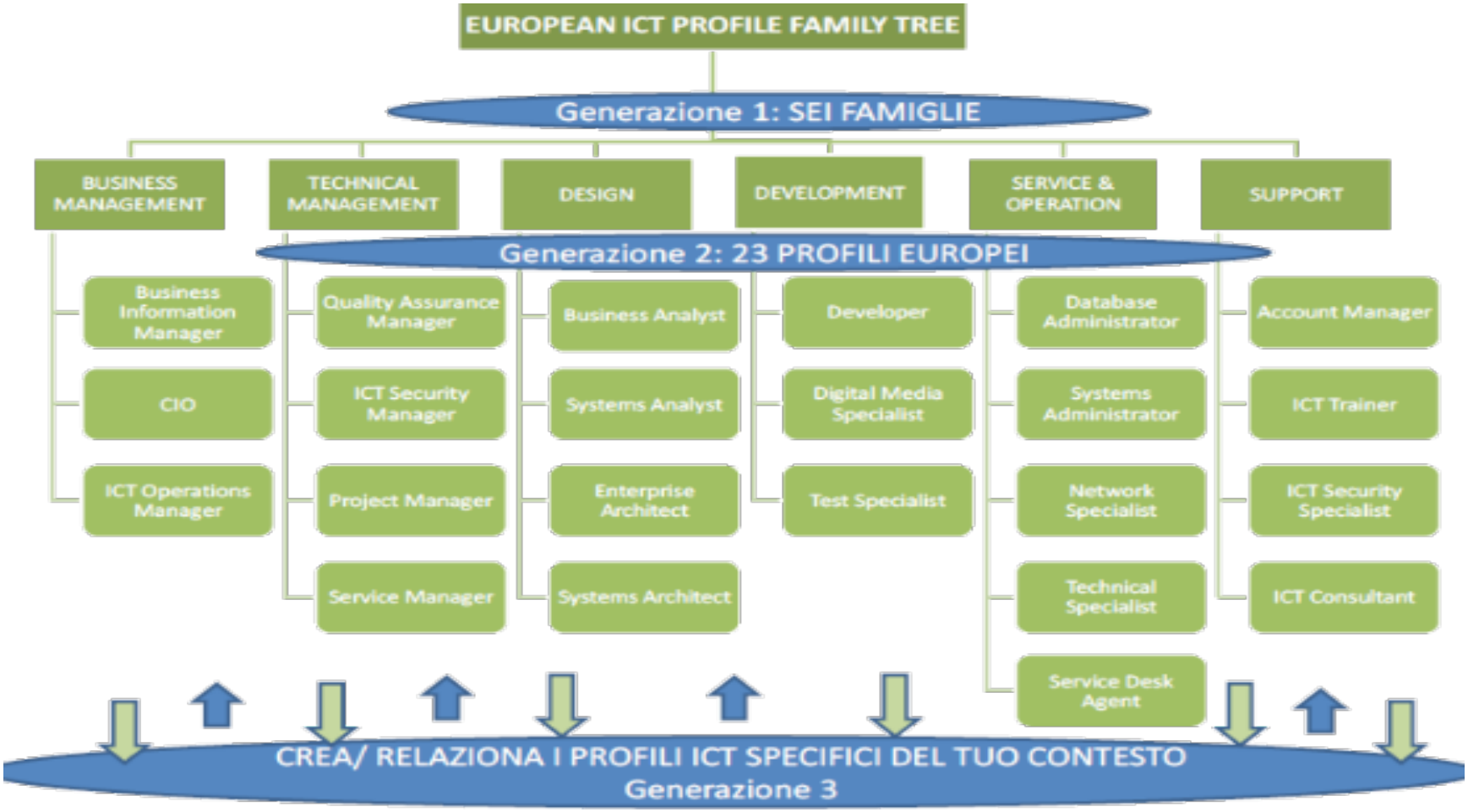
Profili di competenza ICT



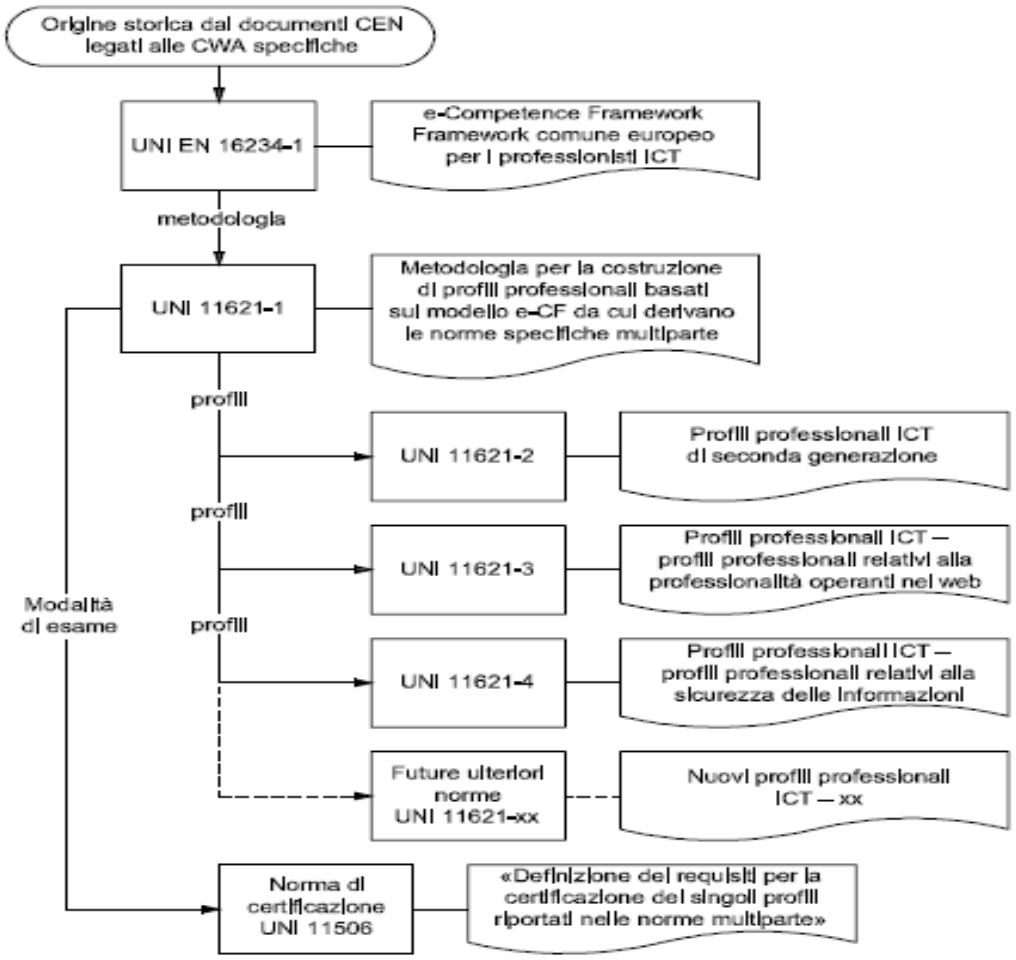
Profili di competenza ICT



Profili di competenza ICT



Le norme tecniche di APNR-ICT



Le norme UNI in ambito APNR – ICT

- **UNI EN 16234-1 –e-Competence Framework (e-CF) - Framework comune europeo per i professionisti ICT in tutti i settori industriali - Parte 1: Framework (modello di riferimento)**

- **UNI 11506:2017 – Attività professionali non regolamentate - Figure professionali operanti nel settore ICT - Requisiti per la valutazione e certificazione delle conoscenze, abilità e competenze per i profili professionali ICT basati sul modello e-CF**

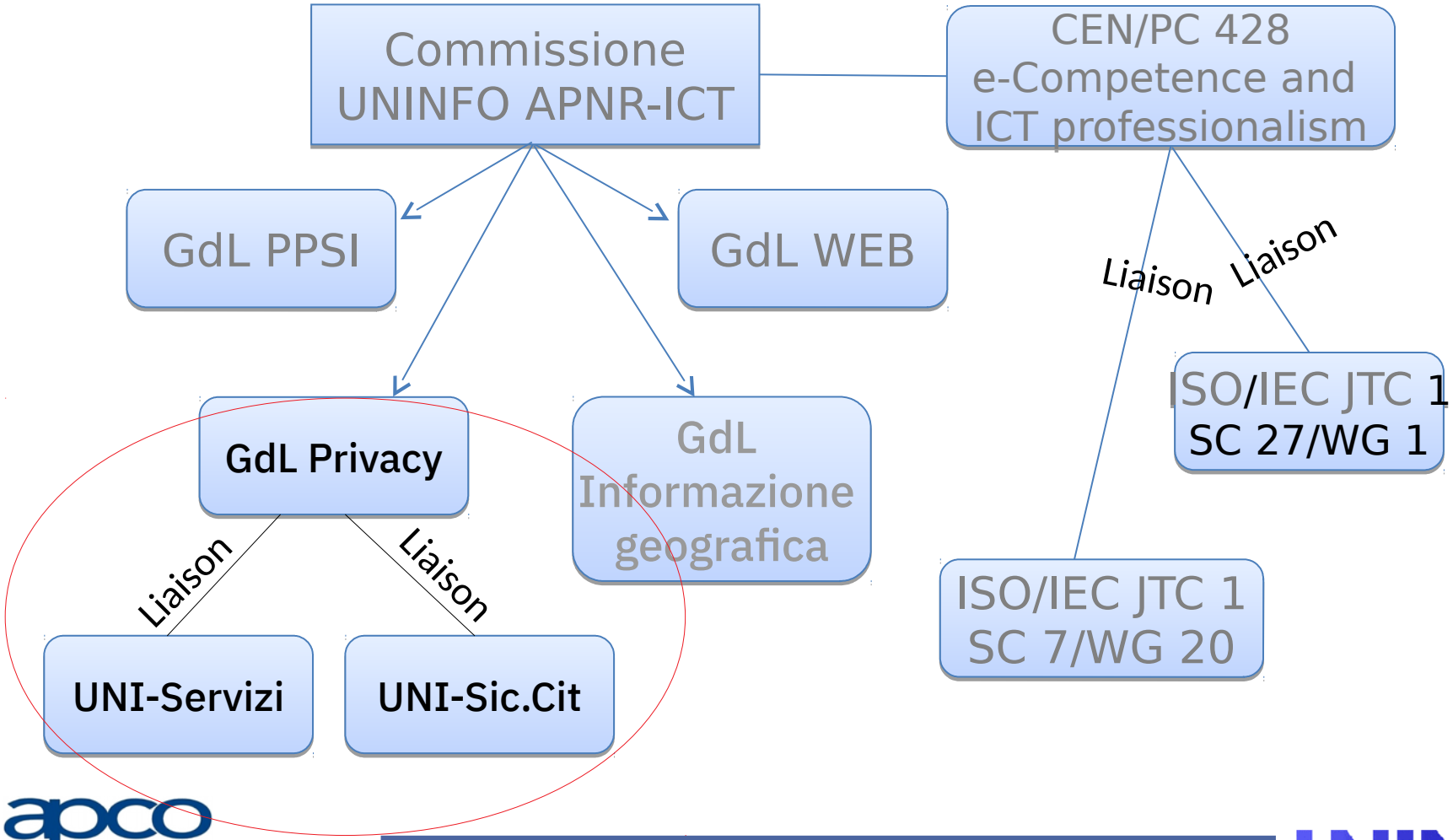
Le norme UNI in ambito APNR – ICT

- UNI 11621:2016 «Attività professionali non regolamentate - Profili professionali per l'ICT»
  - Parte 1 Metodologia per la costruzione di profili professionali basati su sistema e-CF
  - Parte 2 Profili professionali di "seconda generazione"
  - Parte 3 Profili professionali relativi alle professionalità operanti nel Web
  - Parte 4 Profili professionali relativi alla sicurezza delle informazioni

Le norme UNI in ambito APNR – ICT

- **UNI 11697 - Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza**

La UNI 11697...


Commissione UNINFO APNR-ICT
CEN/PC 428 e-Competence and ICT professionalism
GdL PPSI
GdL WEB
Liaison
Liaison
ISO/IEC JTC 1 SC 27/WG 1
GdL Privacy
GdL Informazione geografica
Liaison
Liaison
ISO/IEC JTC 1 SC 7/WG 20
UNI-Servizi
UNI-Sic.Cit

UNI 11697…

… pubblicata il 30 novembre 2017 sui Profili professionali relativi al trattamento e alla protezione dei dati personali e basata su e-CF 3.0

DPO **(completamente allineato al Regolamento)**

Manager privacy

Soggetti con un elevatissimo livello di conoscenze, abilità e competenze in uno specifico contesto organizzativo (sia esso un'area funzionale dell'organizzazione sia il settore di appartenenza della stessa) per garantire l'adozione di idonee misure organizzative nel trattamento di dati personali.

Specialista privacy

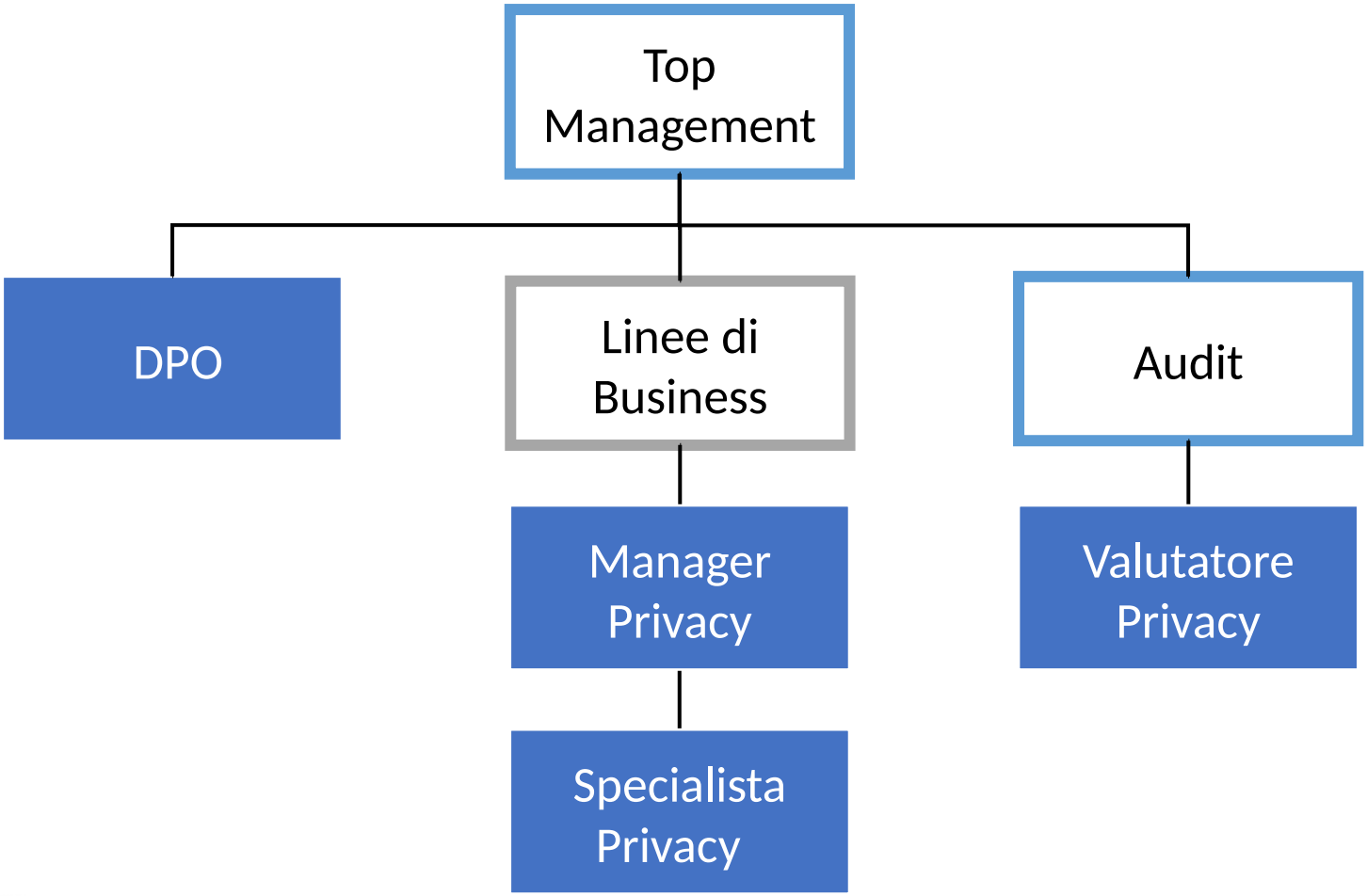
Soggetti che supportano il Responsabile per la protezione dei dati personali e/o il Manager privacy nel mettere a punto le idonee misure tecniche e organizzative ai fini del trattamento di dati personali.

Valutatore privacy

Soggetti indipendenti con conoscenze e competenze nel settore informatico/tecnologico e di natura giuridica / organizzativa che conducono attività del trattamento e della protezione dei dati personali che possono comunque avvalersi di specialisti in entrambi gli ambiti per effettuare attività di audit.

UNI 11697…

Esempio di organizzazione basata sui profili della norma



Profilo del DPO

- E' stato allineato esattamente con quanto richiesto dal Regolamento in termini di task e deliverables
- E' possibile aggiungervi alcuni o anche tutti compiti assegnati al profilo del Manager Privacy

MISSIONE

Fornisce al titolare/responsabile del trattamento il supporto indispensabile ad assicurare l'osservanza del Regolamento UE 2016/679.

COMPETENZE

E-CF 3.0	*Livello*
A.4. Pianificazione di Prodotto o 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

Profilo del Manager Privacy

- E' coerente rispetto alle figure di più alta responsabilità che già oggi si occupano di protezione dei dati personali

MISSIONE

Coordina trasversalmente i soggetti coinvolti nel trattamento dei dati personali, al fine di garantire il rispetto delle norme di legge applicabili e il raggiungimento nonché il mantenimento del livello di protezione adeguato in base allo specifico trattamento di dati personali effettuato, coordinando trasversalmente i soggetti in essi coinvolti.

COMPETENZE

E-CF 3.0	*Livello*
A.4. Pianificazione di Prodotto o di Servizio	3
C.1. Assistenza all'Utente	3
A.5. Progettazione di Architetture	4
D.1. Sviluppo della Strategia per la Sicurezza Informatica	4
D.8. Gestione del Contratto	3
D.9. Sviluppo del Personale	3
D.10. Gestione dell'Informazione e della Conoscenza	5
E.3. Gestione del Rischio	4
E.8. Gestione della Sicurezza dell'Informazione	3
E.9. Governance dei Sistemi Informativi	4

Profilo dello Specialista Privacy

- Rappresenta il grosso del personale competente in materia di protezione dei dati personali

MISSIONE

Svolge le attività operative che si rendono progressivamente necessarie durante tutto il ciclo di vita di un trattamento di dati personali collaborando con una figura manageriale (quale, per esempio, il manager privacy competente).

COMPETENZE

E-CF 3.0	*Livello*
A.5. Progettazione di Architetture	3
A.6. Progettazione di Applicazioni	1
B.5. Produzione della documentazione	1
C.1. Assistenza all'Utente	2
C.2. Supporto alle modifiche/evoluzioni del sistema	3
D.9 Sviluppo del personale	2
D.10. Gestione dell'Informazione e della Conoscenza	3
E.3. Gestione del Rischio	2
E.8. Gestione della Sicurezza dell'Informazione	2

Profilo del Valutatore Privacy

- Rappresenta la terza parte esterna per eccellenza
- Deve rimanere indipendente dalle altre figure

MISSIONE

Esamina periodicamente il trattamento di dati personali, valutando il rispetto di leggi e regolamenti applicabili e approva le misure necessarie a eliminare eventuali non-conformità rilevate, mantenendo una posizione indipendente da chi svolge attività manageriali e operative.

COMPETENZE

E-CF 3.0	*Livello*
A.5. Progettazione di Architetture	3
A.6. Progettazione di Applicazioni	1
B.5. Produzione della documentazione	2
D.10. Gestione dell'Informazione e della Conoscenza	4
E.3. Gestione del Rischio	2
E.5. Miglioramento del Processo	4
E.8. Gestione della Sicurezza dell'Informazione	2

Agenda

- Norme tecniche
  - Cosa sono, chi le sviluppa, benefici
- UNI ed UNINFO
- APNR/ICT
  - UNI EN 16234
  - UNI 11697
- Certificazione UNI 11697?

Percorso di certificazione ...

Apprendimento formale (**istruzione**)

Apprendimento non formale (**formazione professionale**)

Apprendimento informale (**esperienza lavorativa**)

Valutazione delle competenze e certificazione delle competenze

Mantenimento e rinnovo

Requisiti minimi di accesso

Certificazione delle persone nel GDPR?

Certificazione delle persone nel GDPR?

Articoli 42 & 43 GDPR – Certificazione

- ✓ Rilasciata da organismi di certificazione o dall'autorità di controllo competente sulla base di criteri approvati dall'autorità di controllo competente o dal Comitato
- ✓ Utilizzabile volontariamente da titolari e responsabili
- ✓ Con validità massima di 3 anni
- ✓ Inerente alle attività di trattamento*
- ✓ 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
- ✓ Gli organismi di certificazione devono essere accreditati dall'autorità di controllo competente o dall'ente di accreditamento nazionale conformemente alla norma ISO/IEC 17065:2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente

Certificazione delle persone nel GDPR?

Gli articoli 42 e 43 sono applicabili anche alle certificazioni delle persone?

Il "common understanding" attuale propende verso una risposta negativa ma non esiste una risposta ufficiale. Nel frattempo il Garante ha rilasciato il seguente comunicato congiuntamente con Accredia il 18/07/2017:

> *Regolamento Ue e certificazione in materia di dati personali*
> *ACCREDIA e il Garante per la protezione dei dati personali ritengono necessario sottolineare - al fine di indirizzare correttamente le attività svolte dai soggetti a vario titolo interessati in questo ambito - 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 2016/679", poiché devono ancora essere determinati i "requisiti aggiuntivi" ai fini dell'accreditamento degli organismi di certificazione e i criteri specifici di certificazione.*

Requisiti minimi di accesso definiti nella UNI 11697

	Titolo di studio	Formazione specifica	Esperienza lavorativa
DPO/ Responsabile protezione dati	Laurea	80 ore	6 anni (4 manageriali)
Manager privacy	Laurea	60 ore	6 anni (3 manageriali)
Specialista privacy	Diploma	24 ore	4 anni
Valutatore privacy	Diploma	40 ore	6 anni (3 audit)

Schema di certificazione Accredia

Il 12 febbraio 2018, Accredia ha pubblicato le Disposizioni in materia di certificazione e accreditamento per la conformità alla norma UNI 11697:2017, che uniformano rispetto a tutti gli enti di certificazione:

- i requisiti di competenza degli esaminatori e dei candidati
- i meccanismi di conseguimento multiplo, transizione e rinnovo
- le seguenti modalità di svolgimento dell'esame oltre all'esame del CV

RPD/DPO	Prova scritta da 40 domande a risposta multipla e 3 casi studio Esame orale da almeno 40 minuti
Manager privacy	Prova scritta da 35 domande a risposta multipla e 3 casi studio Esame orale da almeno 40 minuti
Specialista privacy	Prova scritta da 35 domande a risposta multipla e 2 casi studio Esame orale da almeno 30 minuti
Valutatore privacy	Prova scritta da 35 domande a risposta multipla e 2 casi studio Esame orale da almeno 30 minuti

A chi serve davvero una certificazione

Al momento la risposta potrebbe essere "TUTTI" per avere una guida univoca all'applicazione dei requisiti del Regolamento e non quella definita dal consulente di turno.

A tendere la risposta potrebbe essere:

- PMI, soprattutto "P"
- fornitori di servizi che vogliono distinguersi sul mercato
- fornitori di prodotti che producono che vogliono distinguersi sul mercato
- soggetti che sono stati oggetto di violazione

Ricordiamo comunque che la certificazione resta su base volontaria e non si sa come sarà valutata dall'autorità di controllo.

Follow us on:
www.uninfo.it

https://www.facebook.com/UNINFO.it
https://twitter.com/uninfo_it
http://www.slideshare.net/uninfoit

Grazie dell'attenzione

Segreteria UNINFO
uninfo@uninfo.it