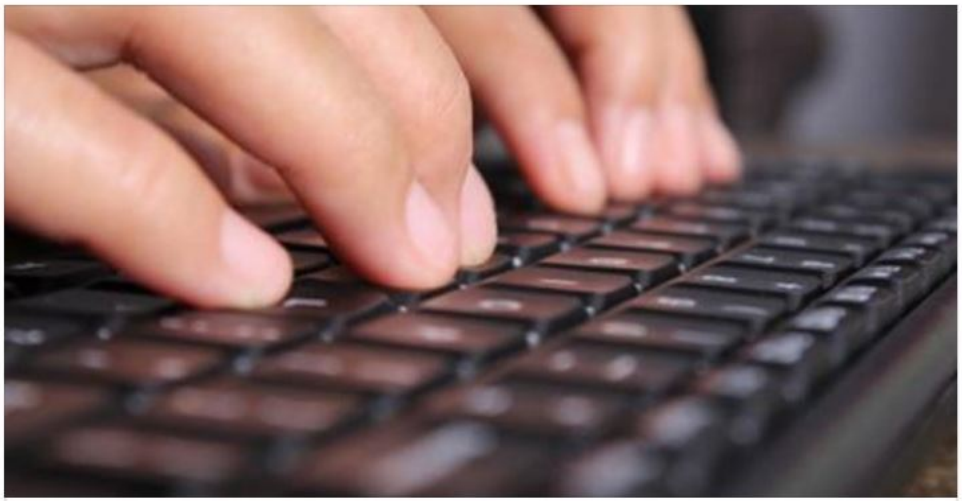
I professionisti della digitalizzazione e della privacy: uno sguardo d'insieme

Avv. **Andrea Lisi**

L’era dei «nativi digitali»

…e ancora oggi ci stupiamo se l'email ha valore legale?



Consulenza legale: se invii una mail a un avvocato devi pagarlo

L'email è una valida prova che dimostra il conferimento dell'incarico all'avvocato perché l'opera professionale si presume a titolo oneroso e non gratuito.

LALEGGEPERTUTTI.IT

Cass. sent. n.1792/17 del 24.01.17

Purtroppo il nostro rapporto con la tecnologia è fermo a questo modus operandi…

E anche il rapporto con il diritto,
con le informative, i contratti
è fermo a questo punto…

E in fatto di protezione dei dati e di gestione sicura del proprio patrimonio informativo stendiamo un velo pietoso…

I ministeri italiani sotto attacco degli hacker - L'Espresso

espresso.repubblica.it/inchieste/2017/02/13/news/i-ministeri-italiani-sotto-attacco-degli-hacker-1.295315

NETWORK ACCEDI ABBONATI

L'Espresso

Cerca

HOME INCHIESTE PALAZZO ATTUALITÀ AFFARI INTERNAZIONALE VISIONI OPINIONI BLOG FOTO VIDEO

Sei in: HOME > INCHIESTE > I ministeri italiani sotto attacco...

Pinterest Email

ESCLUSIVO

I ministeri italiani sotto attacco degli hacker

Oltre agli Esteri anche la Difesa e la rappresentanza italiana alla Ue: la cyber intrusione si è protratta almeno per tutto il 2016. Tutta la rete, ambasciate comprese, è stata bucata. Una feroce offensiva dal danno incalcolabile. Che le autorità hanno preferito nascondere. E che ora l'Espresso vi rivela

DI FLORIANA BULFON

13 febbraio 2017

0 FACEBOOK TWITTER PINTEREST GOOGLE

Le intrusioni di hacker al ministero degli Esteri, ma anche alla Rappresentanza italiana a Bruxelles e alla Difesa sono continue. La nostra

In attesa di risposta da www.facebook.com...

13:17 02/05/2017

Insicurezza reale?

InTime
Condivido per Comunicare

itasascom
Innovation | Digital Transformation | Advanced Analytics
SCARICA ORA IL MAGAZINE
sas

News · Social Media · E-commerce · Events&WebMarketing · Web&Tech · Mobile Tech · Startup Business

Cybercrime: in Italia il fenomeno dei reati informatici è cresciuto del 51% in 5 anni

Franz Russo · 5 luglio 2017 · Security & Privacy · Lascia un commento

201 CONDIVISIONI

In 5 anni il fenomeno del Cybercrime, reati informatici, in Italia è cresciuto del 51%. E' quanto emerge da un'analisi condotta da DAS. In rapporto alla popolazione, il fenomeno è più diffuso in Liguria mentre la Puglia è la regione con la più bassa densità di reati di questo tipo.

Una ricerca condotta da DAS, compagnia di Generali Italia specializzata nella tutela legale, evidenzia come il fenomeno del Cybercrime, i reati informatici, sia cresciuto in Italia, in 5 anni (dal 2010 al 2015), del 51%. La ricerca permette anche di conoscere quanto il fenomeno abbia colpito le nostre regioni. E quindi, la Liguria, con una denuncia all'autorità giudiziaria (per "truffe e frodi informatiche" e delitti "informatici") ogni 246 abitanti, è la regione italiana con la più elevata frequenza di reati informatici, seguita da Molise (con 1 denuncia ogni 290 residenti) e Valle d'Aosta (1/294).

SHOPWIKI

Trovaci su Facebook

InTime - Blog

PA DIGITALE · INDUSTRIA 4.0 · DIGITAL · TLC · IT WORLD · E-PAYMENT · CLOUD · JOB & SKILL · TECH ZONE · E-HEALTH · START UP · L'EUROPA CHE VERRA' · MEDIA · SMART CITY · PROTAGONISTI · ICT&LAW · PUNTI DI VISTA

HOME » DIGITAL » Cybercrime, stretta dell'Europa: aziende obbligate a segnalare gli attacchi

cerca nel sito · COR.COM · GOOGLE

Like 23 · Tweet · G+1 0 · Share 14

LA DIRETTIVA

Cybercrime, stretta dell'Europa: aziende obbligate a segnalare gli attacchi

L'Europarlamento approva la direttiva in materia di sicurezza informatica: più forte l'azione di monitoraggio e difesa. Ora la palla passa al Consiglio Ue. Dal fenomeno ogni anno stimati danni in 260-340 miliardi di euro

di F.Me

Le società che forniscono servizi indispensabili e operano nei settori bancario, energetico, dei trasporti e della sanità dovranno migliorare la proprie capacità di resistere ai cyber attacchi. Lo ha stabilito oggi la commissione Mercato interno del Parlamento europeo, che ha approvato quasi all'unanimità (34 voti favorevoli, 2 contrari) le nuove norme in materia di sicurezza informatica sulle quali il 7 dicembre era già stato raggiunto un accordo informale tra Parlamento, Consiglio e Commissione.

Anche alcuni fornitori di servizi su internet, come i negozi online (ad esempio eBay e Amazon), i motori di ricerca (come Google) e i cosiddetti "cloud' dovranno adattarsi alle nuove norme sulla cybersecurity. Le aziende avranno l'obbligo di sorvegliare le proprie infrastrutture e segnalare agli Stati membri tutti gli incidenti gravi subiti.

Le uniche ad essere escluse dall'applicazione della direttiva saranno le micro e piccole imprese informatiche. Il testo dovrà ora essere approvato formalmente dal **Consiglio Ue** e dal **Parlamento**,

L'editoriale

di Gildo Campesato

Apple tax, lezione per l'Europa digitale

Il caso della Mela dimostra come il tema fiscale vada affrontato a livello Ue. Serve presto un'armonizzazione delle norme

Ultimo Numero

COR.COM

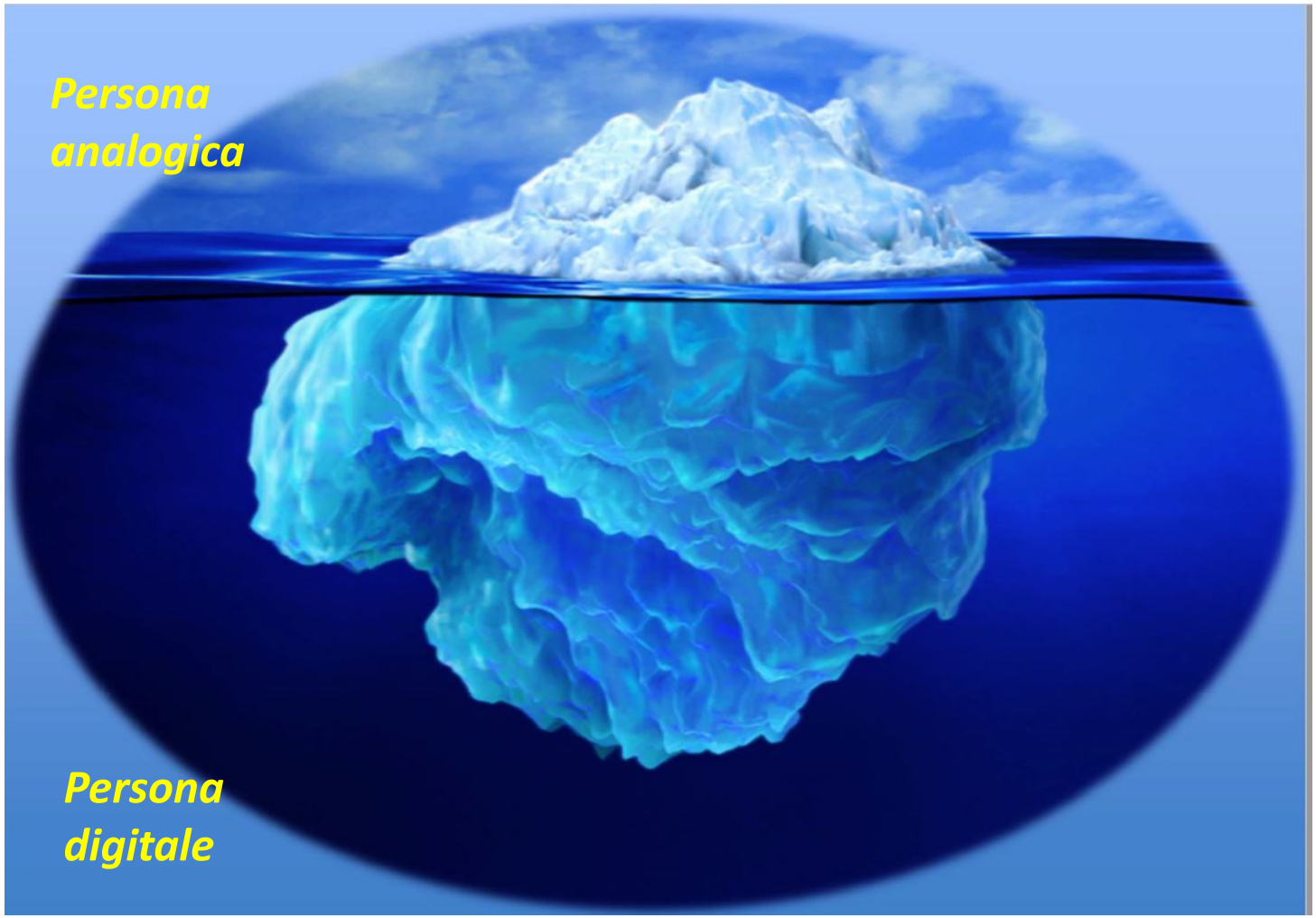
PRIVACY

IL GRANDE BUSINESS

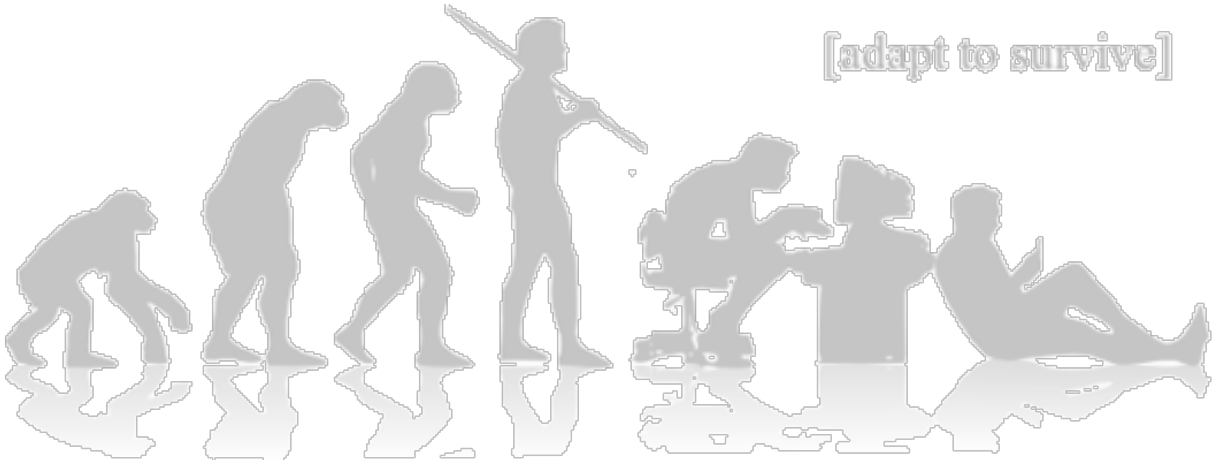
Archivio giornale

MSC CROCIERE

Sicurezza di quali dati e documenti..?



Ormai ci siamo evoluti (o involuti) in una nuova dimensione sociale dove non «possediamo» più i nostri dati e documenti



Ed è «digital first»
(ci piaccia o non ci piaccia)
art. 1 della legge 7 agosto 2015, n.124

- Il **documento informatico ha pieno valore legale** e addirittura è scelta obbligata per la PA (ma anche per professionisti e imprese)
- Le PA devono sviluppare **processi di gestione elettronica dei documenti**
- I cittadini hanno **diritto di inviare istanze e autodichiarazioni alle PA in modalità digitali**
- La **fatturazione elettronica è obbligatoria** verso la PA ed è un'opportunità via via più necessaria per il mondo privato
- Le **firme e i contratti sono inseriti ormai abitualmente in flussi telematici** (e anche in scambi digitali riversati in contesti sempre più dinamici e social)
- Ormai si va sempre di più verso una **gestione automatizzata e pervasiva di dati, documenti e informazioni**… e occorre fare i conti con le nuove pretese della «**accountability**», della «**privacy by default**» e «**privacy by design**» contenute nel Regolamento UE 679/2016
- **Il mondo è digitale**… chi non organizza la propria struttura in ottica digitale sarà fuori dal sistema in poco tempo
- Per gestire questo processo **non ci si può improvvisare**…ma occorre rivedere strategie, modelli organizzativi, competenze. In poche parole: **dobbiamo riorganizzare il nostro modo di stare al mondo**.

I documenti cartacei sono e saranno sempre di più una fastidiosa e residuale eccezione

Il documento informatico non è “carta informatica”:

- «**documento elettronico**»: qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva (Regolamento eIDAS - REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE)
- «**documento informatico**»: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, comma 1°, lett.p, del CAD, di cui al D.Lgs. 82/2005, modificato dal D.Lgs. 179/2016 e dal D. Lgs. 217/2017)
- Quindi, il documento informatico è una **registrazione affidabile e durevole di dati giuridicamente rilevanti**

I documenti amministrativi informatici

- **Art. 23 ter CAD** : “Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge”.
- Ai sensi dell’art. **40 del Codice dell’Amministrazione Digitale comma 1**, le PA formano gli originali dei propri documenti e registri con mezzi informatici secondo le disposizioni del codice e delle regole tecniche in vigore, **senza eccezioni**.

Le **fonti giuridiche della digitalizzazione documentale e della protezione dei dati**:

Le principali norme che ci interessano

- **Codice della Amministrazione Digitale** (D. Lgs. 82/2005)
- «**Codice della privacy»** (Allegato B del D. Lgs. 196/2003)
- **Codice dei beni culturali** (D. Lgs. 42/2004)
- **DPR 445/2000** (Testo Unico sulla documentazione amministrativa)
- **DPCM 13 novembre 2014** (Regole tecniche sul documento informatico)
- **DPCM 3 dicembre 2013** (Regole tecniche sul protocollo informatico)
- **DPCM 3 dicembre 2013** (Regole tecniche sulla conservazione dei documenti informatici)
- **DPCM 22 febbraio 2013** (Regole tecniche su firma digitale e firma elettronica avanzata)
- **DPR 11 febbraio 2005 n. 68** (Posta Elettronica Certificata)
- **D.Lgs. n. 33/2013** (Trasparenza amministrativa)
- **DMEF 17 giugno 2014** (Conservazione digitale documenti fiscali)
- **D.Lgs. 20 febbraio 2004 n. 52** (Fattura elettronica)
- **Circolare Agenzia delle Entrate n. 45/E** (del 19/10/2005)
- **Circolare Agenzia delle Entrate n. 36/E** (del 06/12/2006)
- **Direttiva 45/2010/UE del 13 luglio 2010** (Legge n. 228/2012)
- **Circolare AE 12/E del 3 maggio 2013** (…)

Le altre normative di riferimento

Libro Unico del Lavoro:

Legge 133/2008 (conv. D.L. 112/2008) – artt. 39-40

Decreto Ministero Lavoro 9 luglio 2008

Circolare n. 20/2008 Ministero Lavoro 21/08/2008 + Note Inail 26/08/2008 e 10/09/2008

Registri e contratti assicurativi:

Regolamento ISVAP n. 27 del 14 ottobre 2008 *(in vigore dal 1° luglio 2009)*

Regolamento ISVAP n. 34 del 19 marzo 2010 *(in vigore dal 15 luglio 2010)*

Regolamento IVASS n. 8 del 3 marzo 2015 in materia di semplificazione delle procedure e degli adempimenti burocratici nei rapporti tra imprese, intermediari e clientela

Documenti bancari:

«Assegno elettronico» (DL 70/2011 + DMEF 03.10.2014 n° 205 + Regole Tecniche Banca d'Italia)

Trasparenza operazioni e servizi finanziari – Provv. Banca d'Italia del 15/07/2015 (in vigore dal 1/10/2015)

Gli ultimissimi aggiornamenti che ci riguardano

DECRETI LEGISLATIVI 235/2010 , 179/2016, 217/2017 - Modifiche al Codice dell'amministrazione digitale

Legge di bilancio (L. 205/2018), Legge di delegazione europea (163/2017), Legge europea (167/2017) - Modifiche al Codice per la protezione dei dati personali

Nuove Regole Tecniche

Regolamento eIDAS *(electronic IDentification Authentication and Signature):* Regolamento (UE) N. 910/2014 del PARLAMENTO EUROPEO e del CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE

Regolamento GDPR *(General Data Protection Regulation):* Regolamento (UE) N. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE

Il Codice dell'Amministrazione Digitale

15/02/2015
Piano di informatizzazione D.L. 90/2014 art. 24 comma 3 bis

31/03/2015
Obiettivi accessibilità
Circolare 61/2013 Agid

11/10/2015
Protocollo Informatico
Dpcm 3/12/2013

12 Agosto 2016
Nuove Regole Tecniche Documento Informatico
Dpcm 13/11/2014

11 Aprile 2017
Manuale di Conservazione
Dpcm 3/12/2013

Circolare Agid sulle misure minime di sicurezza
(Circolare 18 aprile 2017, n. 2/2017):
adeguamento entro **31 dicembre 2017**

Le fasi del documento informatico

FORMAZIONE
(originale informatico, copia per immagine, copia informatica, duplicato)

Integrità, immodificabilità, autenticità

Le Regole Tecniche

GESTIONE DOCUMENTALE
(protocollo - registrazione e segnatura di protocollo, classificazione, organizzazione e fascicolazione, assegnazione, reperimento)

Contestualizzazione, archiviazione, ricercabilità

Linee Guida

CONSERVAZIONE
(verifica, consolidamento, mantenimento leggibilità nel tempo, sicurezza)

LA PA CHE ®INNOVA

MODELLO PER LA GESTIONE AUTOMATIZZATA DEI FLUSSI DOCUMENTALI, LA CORRETTA PROTEZIONE, ARCHIVIAZIONE E CONSERVAZIONE A NORMA DEI DOCUMENTI INFORMATICI

INTERAZIONE CON LA PA E SITO WEB ISTITUZIONALE

(CAD, DPCM 13 novembre 2014; L. 241/1990; D. Lgs. 33/2013 e s.m.)

Canali e strumenti per la presentazione delle istanze:

- SITO internet: moduli e formulari online
- PEC id, PEC (e e-mail) + firma digitale *(e firma elettronica qualificata)*
- SPID, CNS e CIE *(firma elettronica avanzata)*

Meccanismi di verifica dei processi:

- Verifica formato
- Verifica della provenienza
- Verifica dell'integrità

Adempimenti agli obblighi di pubblicità legale e trasparenza amministrativa:

- Elenco dei servizi erogati online, accessibili dall'home page del sito istituzionale
- Albo online
- Sezione trasparenza
- FOIA

LA GESTIONE DEL WORKFLOW: IL MANUALE DI GESTIONE INFORMATICA DEI DOCUMENTI

(DPR 445/2000; DPCM 3 dicembre 2013 in materia di protocollo informatico)

Ingresso/produzione del documento con strumenti informatici e avvio delle fase di gestione automatizzata per:

- Trattamento pratiche, verifica procedure e semplificazione procedimenti
- Presupposti per l'avvio del procedimento (Tabella dei procedimenti amministrativi)

Gestione e archiviazione dei documenti:

- Descrizione delle modalità di archiviazione dei documenti inviati, ricevuti, e interni:
- *Registro generale di protocollo e registro giornaliero di protocollo; registri particolari; repertori*
- Definizione del set di metadati per tipologia di documento e caratteristiche del pacchetto di versamento (PdiV)
- Descrizione delle misure adottate per la sicurezza dei sistemi

NB: <u>La corretta archiviazione nel sistema presuppone</u>:

- Classificazione di tutti i documenti (Titolario di classificazione) e quindi assegnazione di una posizione definitiva al documento all'interno del sistema di gestione
- Fascicolazione (Piano per la fascicolatura) per consentire la sedimentazione ordinata nell'archivio e il rispetto del vincolo tra i documenti
- Smistamento e corretta assegnazione all'ufficio competente

CONSERVARE A NORMA: IL MANUALE DI CONSERVAZIONE DEI DOCUMENTI INFORMATICI

(DPCM 3 dicembre 2013 in materia di sistema di conservazione)

Descrizione del modello adottato:

CONSERVAZIONE IN HOUSE

Il soggetto produttore organizza, gestisce e controlla direttamente le procedure conservative all'interno della propria struttura organizzativa

CONSERVAZIONE IN OUTSOURCING

Il soggetto produttore sottoscrive un accordo con un soggetto terzo, pubblico o privato, che eroga il servizio per uno o più soggetti produttori. Il servizio può essere affidato del tutto o in parte all'esterno

Le pubbliche amministrazioni possono rivolgersi esclusivamente a conservatori accreditati, inseriti nell'elenco pubblicato sul sito istituzionale dell'Agenzia.

MISURE DI SICUREZZA LOGICA, FISICA E TECNOLOGICA DEL SISTEMA:

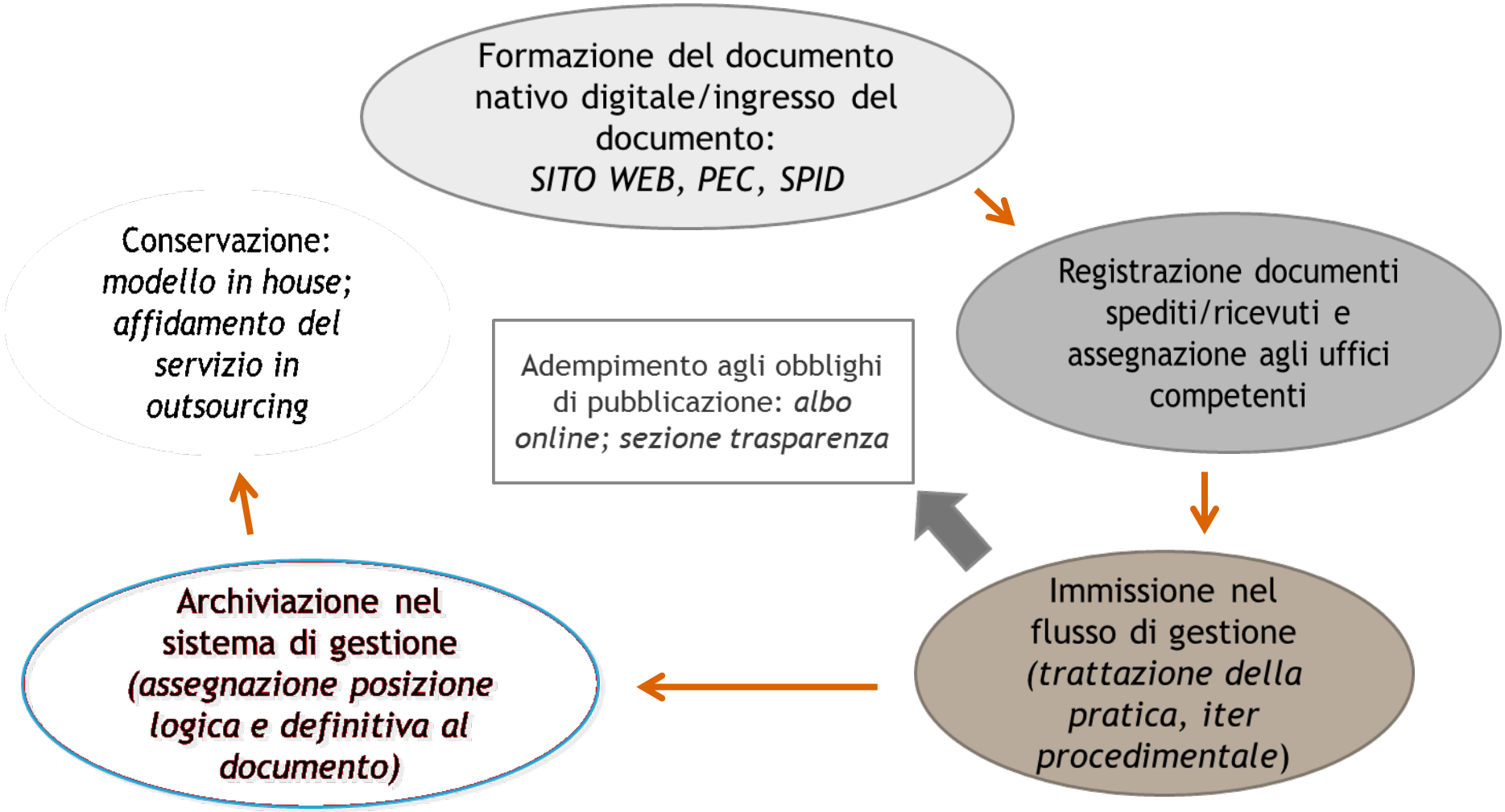
Indice di conservazione definito secondo lo standard UNI 11386:2010 (SInCRO)

Elenco dei formati accettati

Set di metadati per la conservazione, per tipologia di documento

Operazioni di gestione e verifica del funzionamento del sistema nel tempo (monitoraggio continuo, backup e restore)

IL MODELLO DI GOVERNANCE DEI FLUSSI INFORMATIVI E DOCUMENTALI DELLA PA: LE FASI DEL PROCESSO



Principali adempimenti per la PA

Documenti amministrativi da adottare	• Manuale di gestione documentale - DPCM 13 novembre 2014 e 3 dicembre 2013
	• Manuale di conservazione – DPCM 3 dicembre 2013
	• Regolamento per la pubblicazione documenti online
Sistemi di registrazione e archiviazione documentale	• Sistema di protocollo generale conforme alla normativa
	• Ulteriori sistemi di registrazione: censimento dei protocolli particolari e verifica delle caratteristiche
	• Adozione della corretta soluzione di archiviazione documentale
	• Regole tecniche sul protocollo e invio in conservazione del Registro giornaliero di protocollo
Il formato dei documenti amministrativi	• Definizione delle regole di validazione del documento informatico: mappatura del processo di creazione, firme
	• Creazione di documenti informatici validi: mappatura dei processi
	• Verifica degli strumenti di ricezione delle istanze: semplificazione amministrativa nella creazione di form online. Definizione dei livelli SPID
	• Strumenti di ricezione delle istanze online integrati con sistema di archiviazione e con le altre banche dati

Adeguamento delle banche dati

- Verifica del livello di interoperabilità delle banche dati
- Adozione di soluzioni tecnologiche che consentano il dialogo in cooperazione applicativa
- Verifica delle misure di sicurezza adottate a tutela dei dati contenuti, nel rispetto della privacy
- Definizione policy per aggiornamento e pubblicazione dei dati nel rispetto della normativa sulla trasparenza

Individuazione figure professionali

- CDO – Chief Digital Officer (art. 17 del CAD)
- DPO – Digital Preservation Officer
- DPO – Data Protection Officer

Profili tecnici

- Responsabile Trasparenza e pubblicità legale Responsabile Open Data
- Responsabile formazione e gestione documentale
- Responsabile conservazione
- Responsabile della protezione dei dati
- Responsabile della sicurezza informatica e dei sistemi informativi autorizzati

Nuovi profili professionali (e nuove competenze) da sviluppare

La digitalizzazione documentale ha aperto, quindi, la strada all'avvento di

NUOVE FIGURE PROFESSIONALI

deputate a gestire e proteggere informazioni, dati e documenti in formato elettronico

Nuove professioni, attestazioni di qualità, certificazioni professionali: proviamo a fare chiarezza

La legge di riferimento

LEGGE 14 gennaio 2013, n. 4 Disposizioni in materia di professioni non organizzate (in ordini o collegi) - (GU Serie Generale n.22 del 26-01-2013) - Entrata in vigore del provvedimento normativo: 10/02/2013

Possibilità di essere rappresentati da associazioni, senza alcun vincolo di rappresentanza esclusiva

Il Decalogo del DPO (e dei professionisti della digitalizzazione o della privacy)

1) Il **DPO o Responsabile della protezione dei dati è un ruolo**, (o ancora meglio una funzione aziendale o amministrativa), non una vera e propria professione.

2) Esso **viene designato "in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti" previsti dalla normativa europea** (gli articoli di riferimento sono 37-39 del Regolamento)

3) Per sviluppare questa attività **non c'è bisogno necessariamente di bollini di qualità, attestazioni, corsi "abilitanti", iscrizione ad associazioni** o simili.

Il Decalogo del DPO (e dei professionisti della digitalizzazione o della privacy)

4) Frequentare un buon **Corso/Master in materia di digitalizzazione o protezione dei dati** è un'opportunità di aggiornamento e iscriversi a un'associazione rappresentativa (e non «ordinistica») ai sensi della Legge 4/2013 (come ANORC Professioni) può servire a confrontarsi tra professionalità diverse in modo **multidisciplinare**, informarsi con continuità, condividere aggiornamenti e stimolare reti professionali. Ma per qualificarsi "professionista della protezione dei dati" o simili o offrire consulenza in materia **l'iscrizione a un'associazione o la certificazione della professionalità devono sempre e comunque considerarsi facoltative**.

5) Un **professionista iscritto a un Albo, come un avvocato o un ingegnere, non ha necessariamente bisogno di bollini di qualità o certificazioni**. Può ritenersi sufficiente l'appartenenza al suo Ordine professionale che gli comporta un dovere di aggiornamento e di qualità nell'esercizio della professione che esercita.

Il Decalogo del DPO (e dei professionisti della digitalizzazione o della privacy)

6) Oggi esistono **normative UNI** su determinate professioni (richiamate dalla legge 4/2013), le quali consentono a organismi accreditati da Accredia di "certificare" (ai sensi appunto di questa legge sulle professioni non ordinistiche).

7) Le **normative tecniche** (tra cui la "normativa" UNI 11697 sui profili professionali relativi al trattamento e alla protezione dei dati personali o la norma UNI 11536 sulla figura professionale dell'archivista) **non vanno considerate leggi in senso stretto, ma devono intendersi come regolamentazioni facoltative** (e infatti vengono spesso definite "norme volontarie") e non obbligatorie, anche nella descrizione delle professionalità dalle stesse rappresentate.

8) Esistono anche "**standard proprietari**" (quindi "normative tecniche" sviluppate da associazioni o organizzazioni private) su determinate "professioni privacy". Queste consentono in qualche modo di "certificare" ciò che esse stesse privatamente hanno regolamentato. Vanno considerate con attenzione per ciò che sono... e non sempre vengono proposte in modo chiaro.

Il Decalogo del DPO (e dei professionisti della digitalizzazione o della privacy)

9) La prima richiamata **normativa UNI 11697** con le sue categorie professionali in materia di protezione dei dati personali è stata frutto di una scelta criticata dalla maggior parte delle associazioni rappresentative della materia (tra cui ANORC Professioni, Federprivacy, ASSO DPO, Associazione Italiana Difesa Privacy, Istituto Italiano Privacy): purtroppo in alcune occasioni gli standard tecnici seguono strade meno logiche e non sono garantiti in sede di formazione della norma dall'apporto costante di esperti che si occupano con attenzione ed esperienza della materia (e magari si avverte troppo la presenza ingombrante degli stakeholder). Non credo pertanto che questa normativa tecnica UNI (come già successo a quella sugli archivisti sempre di UNI - Norma UNI 11536) avrà molto successo perché è disallineata con la normativa in vigore, non rappresenta le reali esigenze del mercato e soprattutto non riflette le necessità multidisciplinari di una materia così delicata.

10) Lo stesso **Garante italiano della protezione dei dati personali** (con un comunicato stampa del 18 luglio 2017) ha espresso preoccupazione sull'utilizzo sconsiderato delle certificazioni.

Conclusioni

Le certificazioni e le attestazioni di qualità (che le associazioni rappresentative possono rilasciare ai sensi dell'art. 7 della Legge 4/2013) **NON rappresentano un requisito necessario per l'esercizio dell'attività professionale**. Se sviluppate con chiarezza e trasparenza e in modo attento alla qualità, possono essere utili per fornire al Committente una documentazione adeguata sulla propria competenza ed esperienza.

Nulla però può sostituire l'**aggiornamento professionale**, una **adeguata formazione** e una **necessaria esperienza** per svolgere ruoli professionali delicati e soprattutto il **confronto con diverse professionalità**.

MODELLO FUNZIONALE DI GOVERNANCE DI **ANORC PROFESSIONI**

(condiviso nel GdL con Amministrazioni Centrali)

Occorre tener presente che il modello proposto è di tipo FUNZIONALE e NON gerarchico, pertanto l'organizzazione di ruoli e responsabilità deve essere sviluppata coerentemente rispetto a tale principio

GESTIONE DOCUMENTALE

PROTEZIONE DEI DATI PERSONALI

MODELLO FUNZIONALE DI GOVERNANCE: MACROAREE

OPEN DATA, TRASPARENZA E PUBBLICITÀ LEGALE ONLINE

GESTIONE E CONSERVAZIONE DEI DOCUMENTI DIGITALI

TRATTAMENTO DEI DATI PERSONALI NEI SISTEMI DI GESTIONE DOCUMENTALE

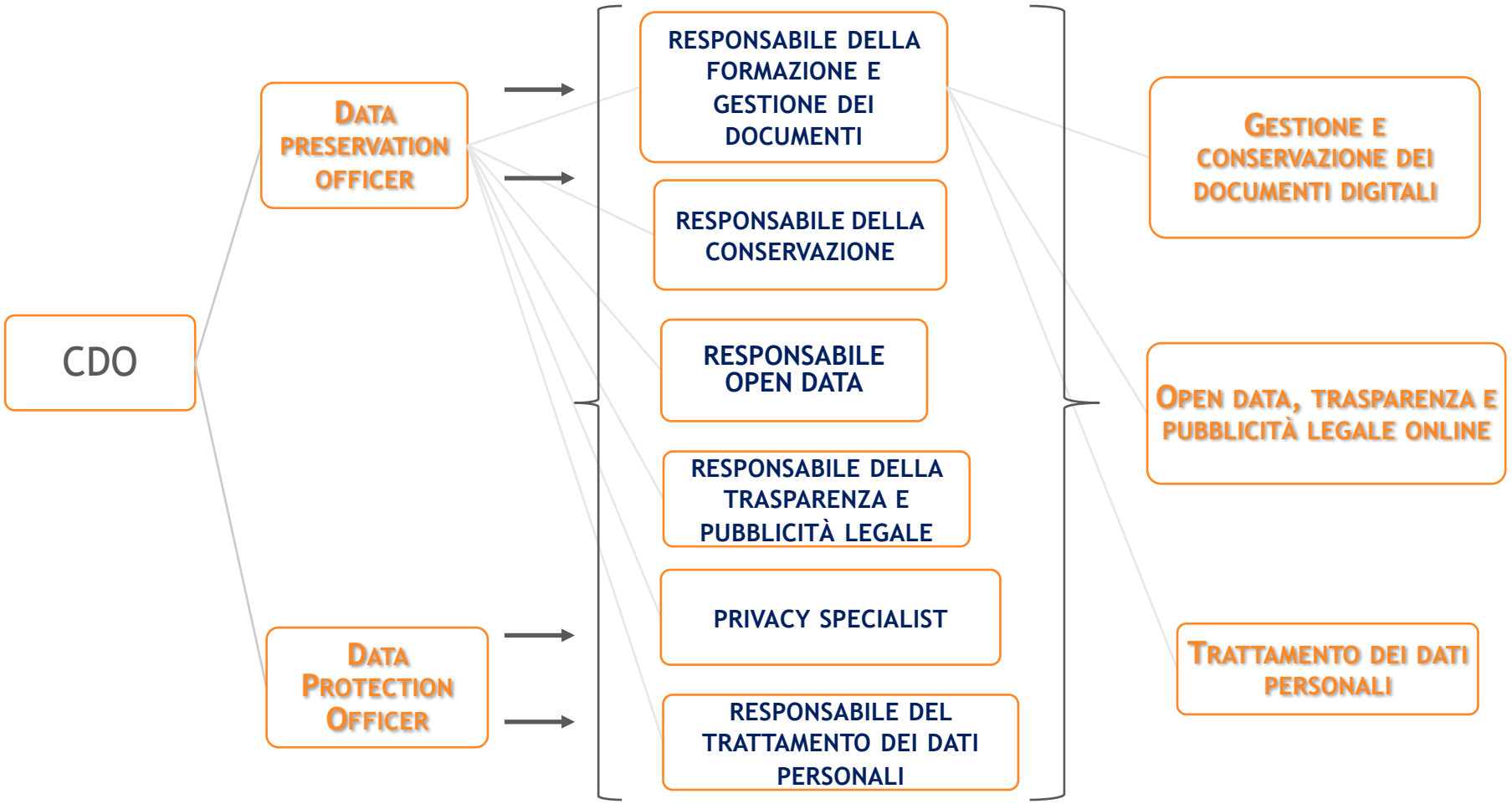
PROFESSIONISTI DELLA DIGITALIZZAZIONE E DELLA PRIVACY

CDO
CHIEF DIGITAL OFFICER O MANAGER DELLA GOVERNANCE DIGITALE (ART. 17 CAD)

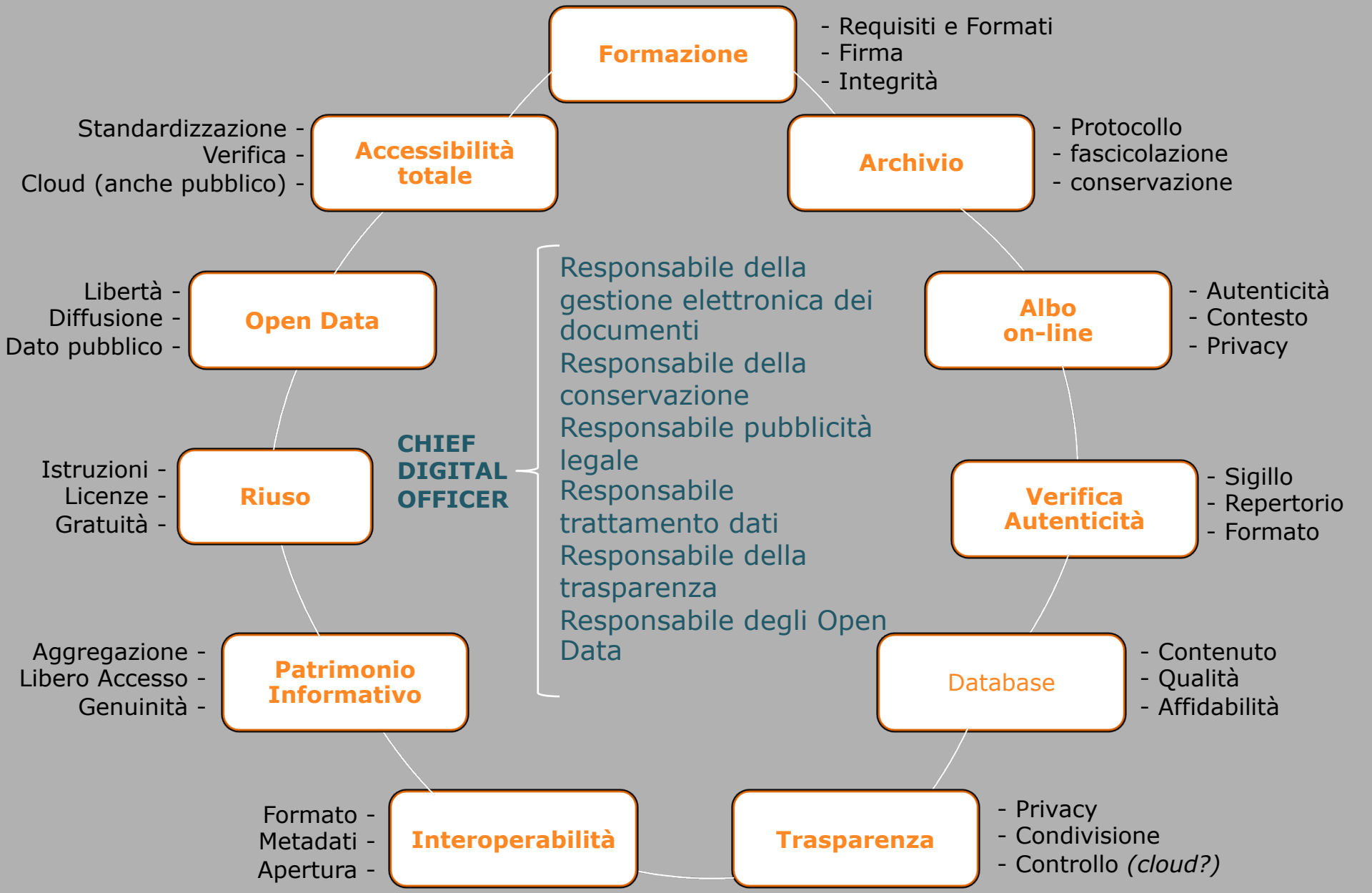
DPO
DIGITAL PRESERVATION OFFICER
O
COORDINATORE DEL CICLO DI GESTIONE DOCUMENTALE

DPO
DATA PROTECTION OFFICER
O
RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

PROFESSIONISTI DELLA DIGITALIZZAZIONE E DELLA PRIVACY



Le fasi del documento informatico amministrativo



eLeadership

- Responsabile della formazione e gestione elettronica dei documenti
- Responsabile della conservazione
- Responsabile pubblicità legale
- Responsabile trattamento dati
- Responsabile della trasparenza
- Responsabile degli Open Data

CONTATTI

Per maggiori informazioni e richiedere le modalità
di **iscrizione ad ANORC Professioni** ecco i nostri contatti:

c/o D&L Department S.r.l.
via Mario Stampacchia, 21
73100 Lecce

Tel e Fax: 0832 25.60.65
Cell: 3277027035

Segreteria: *segreteria.professioni@anorc.it*