

NIS2 e Legge 90/2024 – COA e contratti pubblici

2 OTTOBRE 2024 - AVV. GIUSEPPE VITRANI

Una nuova definizione di enti della pubblica amministrazione

■ Art. 6 n. 35

«ente della pubblica amministrazione»: un soggetto riconosciuto come tale in uno Stato membro conformemente al diritto nazionale, che non comprende la magistratura, i parlamenti e le banche centrali, che soddisfa i criteri seguenti:

- a) è istituito allo scopo di soddisfare esigenze di interesse generale e non ha carattere industriale o commerciale;
- b) è dotato di personalità giuridica o è autorizzato per legge ad agire a nome di un altro soggetto dotato di personalità giuridica;
- c) **è finanziato in modo maggioritario dallo Stato, da autorità regionali o da altri organismi di diritto pubblico**, la sua gestione è soggetta alla vigilanza di tali autorità o organismi, oppure è dotato di un organo di amministrazione, di direzione o di vigilanza in cui più della metà dei membri è designata dallo Stato, da autorità regionali o da altri organismi di diritto pubblico;
- d) ha il potere di adottare, nei confronti di persone fisiche o giuridiche, decisioni amministrative o normative che incidono sui loro diritti relativi alla circolazione transfrontaliera delle merci, delle persone, dei servizi o dei capitali

Il decreto legislativo di recepimento – n. 138 del 4 settembre 2024

ART. 3

Comma 6

Il presente decreto si applica, altresì, anche indipendentemente dalle loro dimensioni, alle pubbliche amministrazioni di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, ricomprese nelle categorie elencate nell'allegato III.

L'allegato III

SCHEMA DI DECRETO LEGISLATIVO DI RECEPIMENTO DELLA NIS2
Attuazione della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di sicurezza informatica nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148

ALLEGATO III

Amministrazioni centrali, regionali, locali e di altro tipo

1. Ai fini dell'articolo 3, comma 6, sono individuate le seguenti categorie:

a) amministrazioni centrali:

- 1) gli Organi costituzionali e di rilievo costituzionale;
- 2) la Presidenza del Consiglio dei ministri e i Ministeri;
- 3) le Agenzie fiscali;
- 4) le Autorità amministrative indipendenti;

b) amministrazioni regionali:

1. le Regioni e le Province autonome.

c) amministrazioni locali

1. le Città metropolitane;
2. i Comuni con popolazione superiore a 100.000 abitanti;
3. i Comuni capoluoghi di regione;
4. le Aziende sanitarie locali.

d) altri soggetti pubblici:

1. gli Enti di regolazione dell'attività economica;
2. gli Enti produttori di servizi economici;
3. gli Enti a struttura associativa;
4. gli Enti produttori di servizi assistenziali, ricreativi e culturali;
5. gli Enti e le Istituzioni di ricerca;



Articolo 1, comma 3, legge 31 dicembre 2009, n. 196

La ricognizione delle amministrazioni pubbliche di cui al comma 2 è operata annualmente dall'ISTAT con proprio provvedimento e pubblicata nella Gazzetta Ufficiale entro il 30 settembre

Ricognizione ISTAT per il 2023

Enti a struttura associativa

Associazione Nazionale Comuni Italiani – ANCI

Associazione Nazionale degli Enti di Governo d'Ambito per l'Idrico e i Rifiuti – ANEA

Centro Interregionale per i Sistemi Informatici Geografici e Statistici in liquidazione – CISIS

Federazione Nazionale dei Consorzi di Bacino Imbrifero Montano – FEDERBIM

Unione delle Province d'Italia – UPI

Unione Italiana delle Camere di Commercio Industria Artigianato e Agricoltura – UNIONCAMERE

Unione Nazionale Comuni Comunità Enti montani – UNCEM



Quindi...da NIS 2
nessuna
conseguenza per gli
Ordini
professionali?

art. 3, comma 7...

Sulla base di un criterio di gradualita', dell'evoluzione del grado di esposizione al rischio della pubblica amministrazione, della probabilita' che si verifichino incidenti e della loro gravita', compreso il loro impatto sociale ed economico, tenuto conto anche dei criteri di cui al comma 9, con uno o piu' decreti del Presidente del Consiglio dei ministri adottati secondo le modalita' di cui all'articolo 40, comma 2, possono essere individuate ulteriori categorie di pubbliche amministrazioni a cui si applica il presente decreto al fine di adeguare l'elenco di categorie di cui all'allegato III.

Anche se l'AgID fornisce risposte interessanti (per altri adempimenti...)

Qual è l'obiettivo per i piccoli enti pubblici non economici a base associativa? Nella scheda non sono contemplati.

L'adempimento non riguarda gli enti pubblici di natura associativa, ai sensi dell'art. 2 comma 2-bis del decreto-legge 31 agosto 2013, n. 101 convertito con modificazioni dalla L. 30 ottobre 2013, n. 125 (come modificato dal decreto-legge 22 giugno 2023, n. 75)

Il nostro consulente in materia di transizione digitale ci ha assicurato che il nostro ente non è tenuto

Il decreto legge 101 del 2013

2-bis. Gli ordini, i collegi professionali, i relativi organismi nazionali e gli enti aventi natura associativa, con propri regolamenti, si adeguano, tenendo conto delle relative peculiarità, ai principi del decreto legislativo 30 marzo 2001, n. 165, ad eccezione dell'articolo 4, del decreto legislativo 27 ottobre 2009, n. 150, ad eccezione dell'articolo 14 nonché delle disposizioni di cui al titolo III, e ai soli principi generali di razionalizzazione e contenimento della spesa pubblica ad essi relativi, in quanto non gravanti sulla finanza pubblica. **Ogni altra disposizione diretta alle amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, non si applica agli ordini, ai collegi professionali e ai relativi organismi nazionali, in quanto enti aventi natura associativa, che sono in equilibrio economico e finanziario, salvo che la legge non lo preveda espressamente.** Per tali enti e organismi restano fermi gli adempimenti previsti dall'articolo 60, comma 2, del citato decreto legislativo n. 165 del 2001

Guardiamo alla catena di fornitura secondo gli atti di esecuzione europei

Politica sulla sicurezza della catena di fornitura:

- Gli enti rilevanti devono stabilire e applicare una politica di sicurezza della catena di fornitura per gestire i rapporti con i fornitori diretti e i prestatori di servizi. L'obiettivo è mitigare i rischi per la sicurezza dei sistemi di rete e informazione.
- La politica deve identificare il ruolo dell'ente nella catena di fornitura e comunicarlo ai fornitori e prestatori di servizi.
- Gli enti devono stabilire criteri per selezionare e contrattare i fornitori, inclusi: le pratiche di sicurezza informatica dei fornitori, la capacità di soddisfare i requisiti di sicurezza informatica specificati, la capacità di diversificare le fonti di approvvigionamento e limitare il "vendor lock-in" (dipendenza da un singolo fornitore).

Guardiamo alla catena di fornitura secondo gli atti di esecuzione europei

Contratti con i fornitori:

I contratti con i fornitori devono includere:

- requisiti di sicurezza informatica
- competenze, formazione e controlli di background dei dipendenti
- obblighi di notifica per incidenti
- diritti di audit e gestione delle vulnerabilità
- disposizioni per subappalti e gestione alla cessazione del contratto.

E quindi....

La direttiva fissa
degli standard

Certamente sono
delle «best
practices»

Possono diventare la
misura dell'accuratezza
nella gestione del
rischio «cyber»?

INOLTRE

Gli Ordini professionali sono clienti di soggetti NIS

(conservatori digitali, fornitori di firme)

Beneficio derivante dall'art. 21 NIS2

ART. 21 NIS 2 (applicabile ai fornitori di servizi fiduciari)

approccio multirischio mirante a proteggere i sistemi informativi e di rete e il loro ambiente fisico da incidenti:

- a) politiche di analisi dei rischi e di sicurezza dei sistemi informativi;
- b) gestione degli incidenti;
- c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;
- d) sicurezza della catena di approvvigionamento
- e) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;
- f) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;
- g) uso di soluzioni di autenticazione a più fattori o di autenticazione continua

L'avvocatura è sulla buona strada?

2024: avvio di servizi di
conservazione digitale per

Negoziazioni
assistite

Mediazioni

CDD

Certamente non si applica l'art. 14 della legge 90 del 2024

Con decreto del Presidente del Consiglio dei ministri, da adottare entro centoventi giorni dalla data di entrata in vigore della presente legge, su proposta dell'Agenzia per la cybersicurezza nazionale, previo parere del Comitato interministeriale per la sicurezza della Repubblica, di cui all'articolo 5 della legge 3 agosto 2007, n. 124, nella composizione di cui all'articolo 10, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, sono individuati, per specifiche categorie tecnologiche di beni e servizi informatici, gli elementi essenziali di cybersicurezza che **i soggetti di cui all'articolo 2, comma 2, del codice dell'amministrazione digitale**, di cui al decreto legislativo 7 marzo 2005, n. 82, tengono in considerazione **nelle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici....**