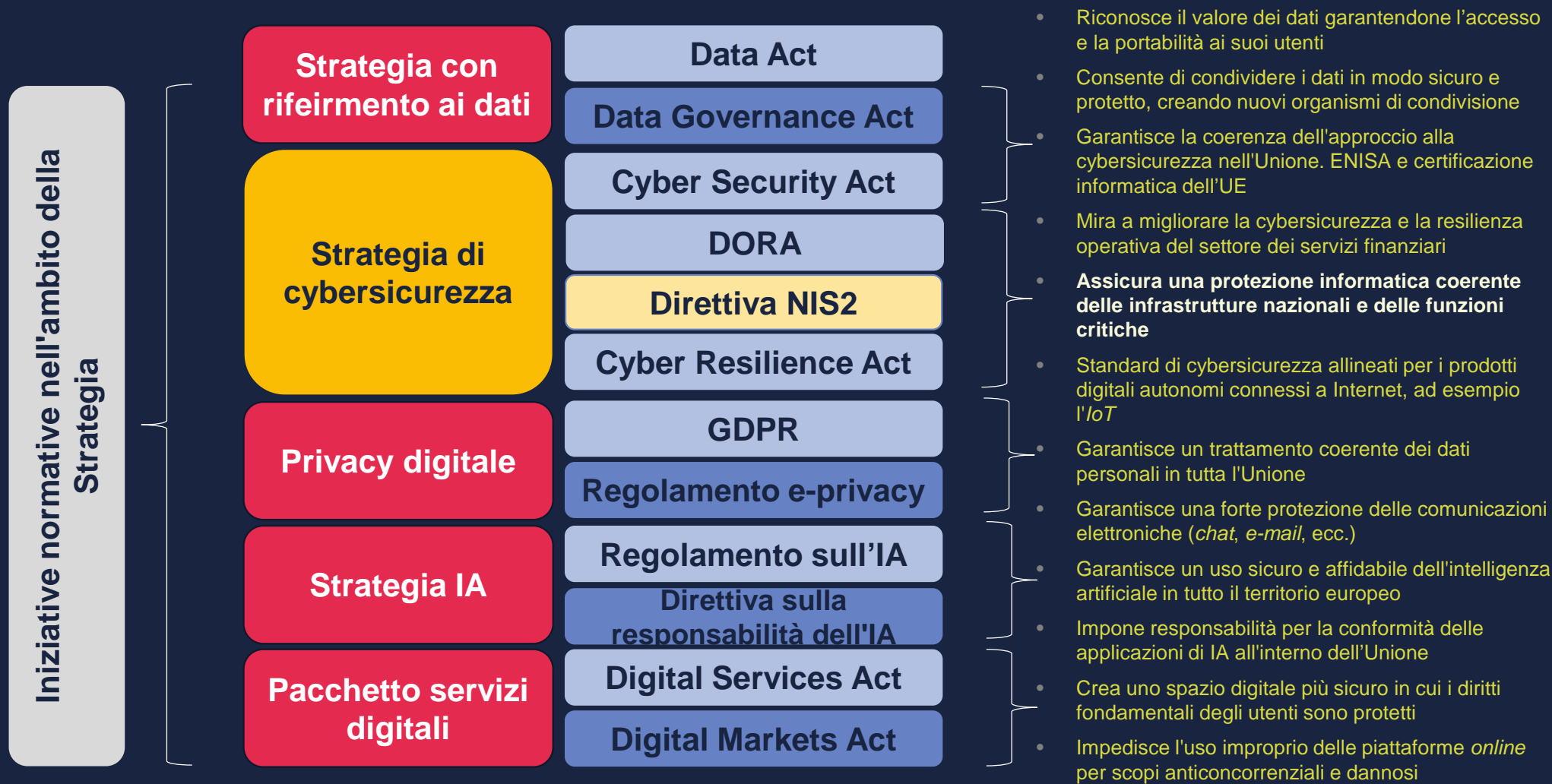


La Direttiva NIS2 è finalmente arrivata – Cosa fare per conformarsi?

La NIS2

Introduzione al Decennio Digitale Europeo

Come si inserisce la NIS2 nella Strategia del Decennio Digitale Europeo?



Calendario per l'adozione della strategia digitale



Che cos'è la NIS2?

Che cos'è la NIS2?

Direttiva sulla sicurezza delle reti e dei sistemi informativi II

- Fa parte della **Strategia di cybersicurezza dell'UE**
- Abroga e sostituisce la **direttiva NIS1 originaria**, entrata in vigore nel 2016
- La NIS2 stabilisce **misure armonizzate di gestione del rischio di cybersicurezza e requisiti di segnalazione per i settori altamente critici**

17 ottobre 2024



Ambito di applicazione della NIS2

La mia società rientra nel campo di applicazione della NIS2?

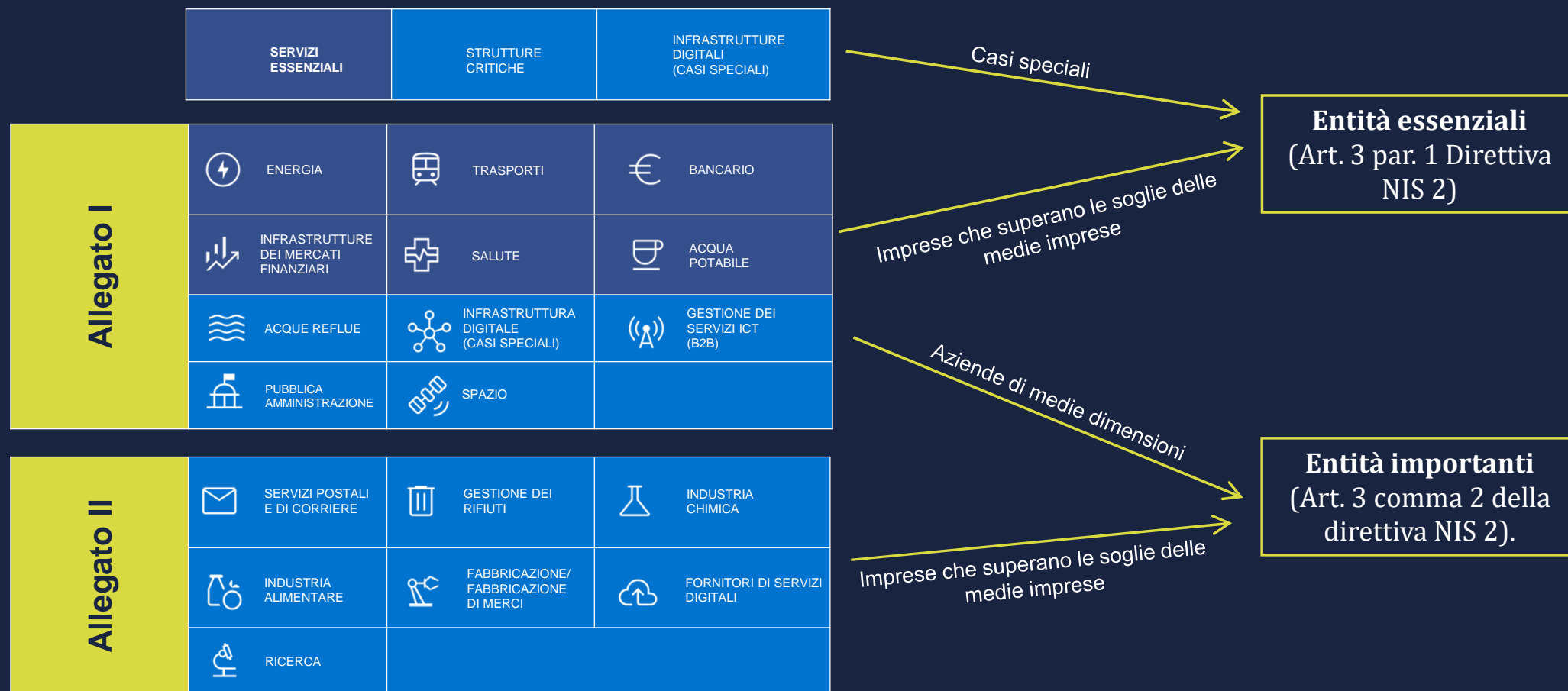


Società che rientrano nei settori dell'Allegato I (Settori ad alta criticità)		
 Energia	Acqua potabile	
 Trasporto	Infrastruttura digitale	
 Settore bancario	Acque reflue	
 Salute	Gestione dei servizi ICT	
 Spazio	Pubblica amministrazione	
	Infrastruttura finanziaria	

Società che rientrano nei settori dell'Allegato II (Altri settori critici)	
Produzione alimentare	
Manfatturiero	
Ricerca	
Posta e corrieri	
Gestione dei rifiuti	
Prodotti chimici	
Fornitori digitali	

La mia società sarà un'entità essenziale o importante?








Questa distinzione è importante quando si considera il grado di applicazione della legge a cui una società può essere soggetta.



Gli elementi chiave della NIS2

Gestione del rischio | Mettere in atto misure di cybersicurezza

Requisiti minimi per le misure nazionali per le aziende per quanto riguarda:

-  **Analisi dei rischi e della sicurezza** dei sistemi informativi
-  **Gestione degli incidenti di sicurezza**
-  **Continuità aziendale** (gestione dei *backup*, *disaster recovery* e gestione delle crisi)
-  **Sicurezza della supply chain**, compresi gli aspetti legati alla sicurezza del rapporto tra le singole società e i loro fornitori diretti o fornitori di servizi
-  Misure di sicurezza nell'**acquisizione, nello sviluppo e nella manutenzione di reti e sistemi informativi**, compresa la gestione e la divulgazione delle vulnerabilità
-  Concetti e procedure per la **valutazione dell'efficacia delle misure di gestione del rischio** nell'ambito della cybersicurezza
-  Uso della **crittografia e delle procedure di multi-autenticazione**, procedure di base nell'ambito dell'igiene informatica, sicurezza delle risorse umane, ecc.

Gestione del rischio - Approvazione e supervisione da parte dell'organo di gestione

Governance e responsabilità per la gestione del rischio di cybersicurezza

- **Gli organi di gestione delle società rientranti nell'ambito di applicazione devono:**
 - approvare le misure di gestione del rischio di cybersicurezza
 - supervisionare la loro attuazione
- Obbligo di **seguire una formazione** sulla gestione del rischio di cybersicurezza

➔ **NIS2 porta la questione della resilienza informatica** fuori dai tech team e nella C Suite

Possibilità per lo Stato membro di imporre all'organo di gestione **una responsabilità**

➔ **personale**

L'autorità competente può imporre un **divieto temporaneo** di esercitare funzioni dirigenziali

➔ **a livello di amministratore delegato o di rappresentante legale (solo per le Entità Essenziali).**

Obblighi di segnalazione | Notifica di incidenti significativi

Garantire che i CSIRT nazionali siano informati in caso di incidenti significativi.

- Obblighi di notifica attivati dal verificarsi di **un incidente significativo**
- L'approccio alla segnalazione di incidenti significativi si articola in tre fasi:
 - 1 **entro 24 ore** dalla prima presa di coscienza - *Report Early Warning*
 - 2 **entro 72 ore** dal momento in cui si è venuti a conoscenza dell'incidente – *Report per l'aggiornamento dell'Early Warning*
 - 3 **entro un mese dalla** notifica iniziale - *Report finale dettagliato*
 - 4 **procedura del CSIRT dopo la ricezione della segnalazione:** *feedback* iniziale sull'incidente significativo, seguito da consigli operativi sull'attuazione di possibili misure correttive

Applicazione e supervisione | Sanzioni

Entità importanti

Importo massimo di 7.000.000 EUR o 1,4% del fatturato globale generato nell'esercizio precedente

→ Si applica l'importo più elevato

Entità essenziali

Importo massimo 10.000.000 di euro o il 2% del fatturato globale generato nell'esercizio precedente

→ Si applica l'importo più elevato

Condizioni generali per l'imposizione delle sanzioni:

- Il livello delle sanzioni deve essere **efficace, proporzionato e dissuasivo**
- Le sanzioni dovrebbero essere comminate **in aggiunta ad** altre misure

Gli elementi da considerare quando si stabilisce una sanzione includono:

- gravità della violazione
- durata
- precedenti di infrazioni
- rilevanza del danno
- dolo o negligenza
- misure di mitigazione adottate
- adesione ai codici di condotta
- livello di cooperazione con le autorità competenti

Attuazione da parte degli Stati membri

A che punto è il recepimento della direttiva da parte degli Stati membri a settembre 2024?

Stato di attuazione del NIS 2

Stato attuale di attuazione negli Stati membri dell'UE

- Sì
- In corso
- No



Preparazione per la NIS2

Quali sono i passi fondamentali che una società deve svolgere per prepararsi alla NIS2?

Cosa possono fare le società per prepararsi?

Determinare **quale Stato membro ha giurisdizione** (solo nel caso di cross-boarder activities)

1

Quale giurisdizione ?

Aggiornamento e preparazione dell'**organo di gestione** in vista di un ruolo più incisivo di monitoraggio della cybersicurezza

5

Preparare l'organo di gestione

Considerare le misure di cybersicurezza

2

Valutare se **le attuali pratiche di gestione del rischio di cybersicurezza** sono sufficienti a soddisfare i requisiti della NIS2

3

Sicurezza della catena di approvvigionamento e contratti

Considerate la supply chain e il relativo livello di cybersecurity dei fornitori

4

Segnalazione di incidenti

Valutare se è possibile **soddisfare gli obblighi di segnalazione della NIS2**

Grazie per l'attenzione



Giulio Coraggio

Partner
Milano, Italia
giulio.coraggio@dlapiper.com



Giulia Zappaterra

Legal Director
Milano, Italia
giulia.zappaterra@dlapiper.com



Cristina Criscuoli

Senior Lawyer
Milano, Italia
Cristina.Criscuoli@dlapiper.com



Edoardo Bardelli

Laywe
Milano, Italia
edoardo.bardelli@dlapiper.com

