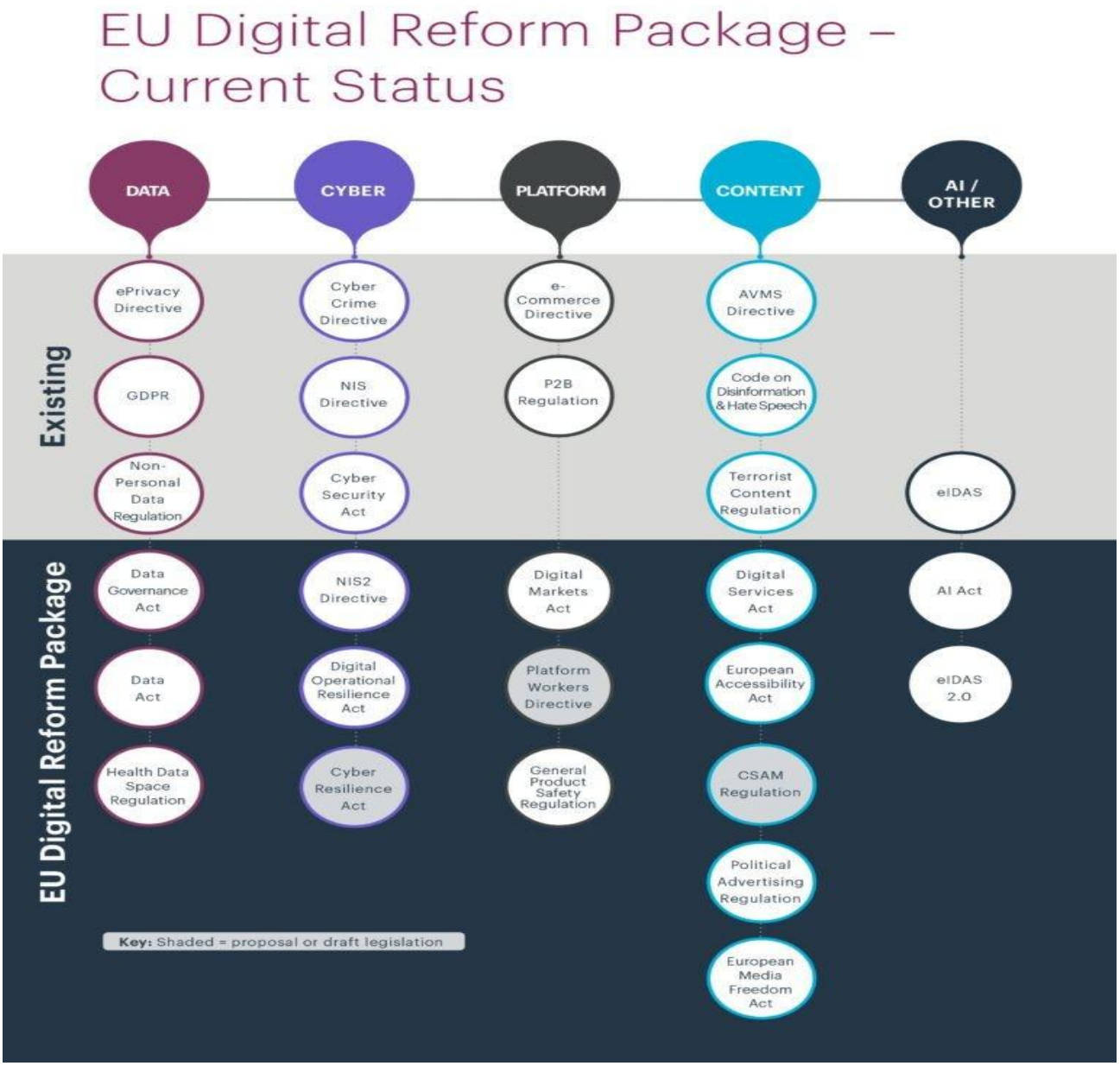
Европейската цифрова супа: Навигация в AI, NIS2, DORA, DSA, DMA и останалите европейски технологични регламенти



Набор от нови цифрови регламенти променят начина, по който организациите изграждат и внедряват технологиите

От новаторския GDPR до наскоро приетия Акт за изкуствения интелект, наред с рамки като Акта за данните, Директивата за сигурността на мрежите и информационните системи

(втора версия) (Directive on Security of Network and Information Systems - NIS2), Регламента за цифрова оперативна устойчивост (Digital Operational Resilience Act - DORA), Акта за цифровите услуги (Digital Services Act – DSA) и Акта за цифровите пазари (Digital Markets Act – DMA), европейският регулаторен пейзаж започва да изглежда като богата, донякъде сложна **„цифрова супа“**. Всеки регламент внася добре обмислени съставки , но за бизнеса получената смес може да доведе до объркване, дублиране на усилия и значителни разходи.

Как стигнахме от GDPR до регулаторна крепост?

За много компании спазването на регулаторните изисквания започна сериозно с GDPR през 2018 г., глобален сравнителен анализ/бенчмарк за поверителност/неприкосновеност на данните, който накара компаниите по целия свят да приемат спазването на изискванията сериозно. Оттогава ЕС непрекъснато добавя нови елементи, като Акта за киберсигурност, Акта за управление на данните, водещи инициативи като Акта за изкуствения интелект, NIS2 и DORA.

Амбицията на ЕС е да изгради единен цифров пазар, основан на доверие и прозрачност.

Защо „супа“? Припокривания и противоречиви изисквания

За разлика от внимателно координирания пакет, тези актове в някои случаи са разработени изолирано. Това означава, че много компании се оказват обект на припокриващи се, а понякога и противоречащи си задължения.

Да разгледаме европейски стартъп, предлагащ платформа за сътрудничество, базирана на изкуствен интелект, с видео, съобщения и интелигентни инструменти за продуктивност. Такъв бизнес може едновременно да се сблъска с:

1. **GDPR** (за обработка на лични данни),
2. **DSA** (ако хостват обществени канали със съдържание, генерирано от потребители),
3. **Акта за изкуствения интелект** (дори за системи с ограничен риск),
4. **NIS2** или **DORA** (ако е част от ИКТ инфраструктура и/или критична инфраструктура).

Тази сложност често води до проблеми със спазването на изискванията.

Например:

GDPR изисква минимизиране на данните, докато ефективните системи с изкуствен интелект процъфтяват с големи набори от данни.

Актът за цифровите услуги (DSA) призовава за алгоритмична прозрачност, която би могла да разкрие поверителна интелектуална собственост съгласно изискванията за техническа документация на Акта за изкуствения интелект.

Какво означава това за една организация?

Отминаха дните, когато спазването на изискванията беше единствено прерогатив на правния екип. Сега ключови роли играят управителните съвети, ИТ, отделите за анализ на данни и отделите за киберсигурност.

Например:

Съгласно **Акта за изкуствения интелект** , организациите може да се нуждаят от оценка на риска, преди да внедрят изкуствен интелект.

Актът за цифровите услуги (DSA) налага многостепенни задължения относно прозрачността и системите за уведомяване и премахване.

NIS2 и **DORA** разшириха мрежата, привличайки дори средно големи фирми в сектори като финанси, здравеопазване и облачни услуги – понякога с пряка отчетност на ниво борд.

Практически стъпки: Превръщане на сложността в стратегия

Въпреки че тази регулаторна „супа“ може да изглежда сложна, има конкретни стъпки, които организациите могат да предприемат:

Определяне кои актове да прилагат

Използване на персонализирани инструменти или консултантски услуги, за определяне кои от приблизително дузината цифрови актове на ЕС са от значение за бизнес модела и операциите.

Един инструмент може да предлага триетапен подход:

- **Оценка на въздействието:** собствената технология създава ясен отчет за това кои актове се отнасят за вас, което помага да се осигури подкрепа от страна на борда.
- **Оценка на готовността:** анализ на пропуските в съществуващите политики и системи.
- **Подкрепа за внедряване:** стратегическо, защитено с привилегии ръководство за запълване на тези пропуски.

Картографиране на системите

Къде се намира изкуственият интелект, какви данни използва и дали се квалифицира като критична инфраструктура съгласно NIS2 или DORA.

- **Разграждане на вътрешните силози**

Насърчаване на сътрудничеството в ранен етап между екипите по правно съответствие, ИТ и AI/ML, за да се откриват конфликтите и да се рационализират процесите.

- **Инвестиране в документация**

Надеждната отчетност и прозрачността са ключови съгласно Акта за изкуствения интелект и GDPR, особено за системите с изкуствен интелект. Това често означава повече оценки на въздействието върху защитата на данните (DPIA) при въвеждането на нови технологии.

- **Външна помощ**

Независимо дали чрез консултантска подкрепа или целенасочено консултиране, външната експертиза може да помогне както на малките и средни предприятия, така и на мултинационалните компании да се справят с тази сложна ситуация по икономически ефективен начин.

По-голямата картина: Геополитика и глобална фрагментация

Тези правила на ЕС не съществуват във вакуум. Нарастващото геополитическо напрежение, опасенията за националната сигурност и различаващите се глобални регулаторни режими формират начина, по който компаниите внедряват продукти с изкуствен интелект и базирани на данни.

Ключови външни фактори :

- **Търговски ограничения:** контролът върху износа на чипове, софтуер и хардуер с изкуствен интелект нарушава веригите за доставки.
- **Контрол на националната сигурност:** повече проверки на чуждестранните инвестиции и забрани за доставчици.
- **Суверенитет на данните:** закони, налагащи локализация на данни и суверенни облачни решения.

- **Фрагментация на регулаторните разпоредби:** различните режими за съответствие (Актът на ЕС за изкуствения интелект, правилата на Китай за изкуствения интелект, изпълнителните заповеди на САЩ) увеличават разходите и сложността.
- **Френдшоринг[1]:** компаниите все по-често изграждат вериги за доставки в рамките на политически обвързани държави.

Така наречените „Брюкселски ефект“ често означава, че компаниите по целия свят следват правилата на ЕС по подразбиране, за да избегнат фрагментиране на операциите, но за някои различаващите се системи все още може да имат смисъл.

Поглед напред: Съответствието като стратегически актив

Голямото послание е: това е само началото!

Основните разпоредби на Акта за изкуствения интелект вероятно ще влязат в сила до 2026 г.

NIS2 и DORA вече имат силна юридическа сила, като по този начин носят лична отговорност на директорите.

Актът за данните, Европейският акт за достъпност, Актът за киберустойчивост и други чакат своя ред.

В тази среда, третирането на съответствието като упражнение за отмятане на квадратчета само по себе си е риск. Компаниите, които гледат на съответствието като на стратегически актив – начин за изграждане на доверие, ускоряване на достъпа до пазара, повишаване на оперативната устойчивост и откроряване пред инвеститорите – не само ще оцелеят, но и ще процъфтяват.

Ключови изводи

Цифровото регулиране на ЕС е тук, за да остане – и то променя начина, по който са проектирани системите, не само начина, по който се използват.

Спазването на правилата вече не е разходен център, то е конкурентен диференциатор. Чрез ранно привеждане в съответствие с тези правила, организациите могат да осигурят бъдещи операции и да получат пазарни предимства. Предвид глобите и санкциите, работата с правилата е по-добра от работата срещу тях.

Не се страхувайте от „супата“ — научете се да работите с нейните съставки. Резултатът ще бъде по-силен и здравословен бизнес, който е в по-добра позиция както за клиентите, така и за регулаторните органи.

https://www.lexology.com/library/detail.aspx?g=55b4ce92-5615-44e2-a812-e33da0fd28cc&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_cam Справочник =Lexology+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2025-07-07&utm_term =

[1] Френдшорингът е нарастваща търговска практика, при която мрежите от веригите за доставки са фокусирани върху държави, считани за политически и икономически съюзници