

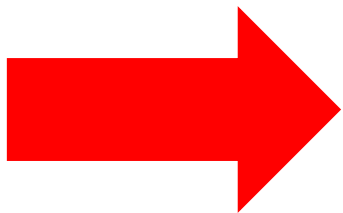
Cybersecurity per piccoli Comuni e le PMI:
sicurezza “a misura di ente”

Carta per fatti o fatti di carta?

Fabio Zanolì NWN SOLUTIONS

*Cosa dovete farci
con la Paper
Compliance...*

Spoiler



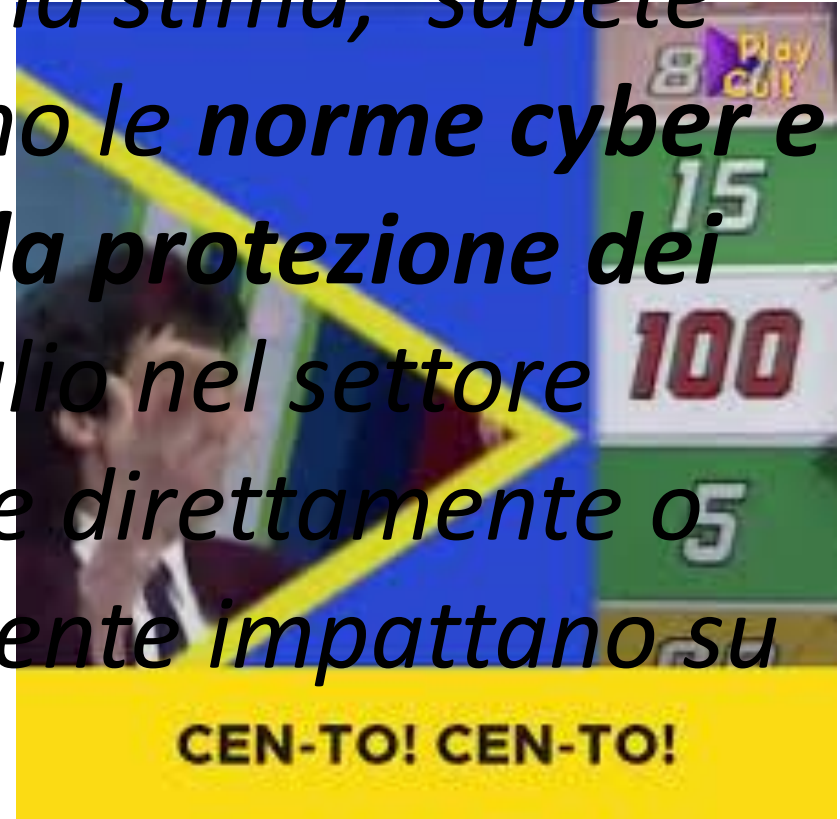


*Fatti non foste per
memorizzar le norme e
farne tomi immani.*

*Ma per farne pratica
d'impresa.*

Dante Alighieri??

*Secondo una stima, sapete quante sono le **norme cyber e relative alla protezione dei dati** o meglio nel settore digitale che direttamente o indirettamente impattano su un ente?*



Recovery and Resilience Facility Regulation, (EU) 2021/241	Frequency Bands Directive, (EEC) 1987/372	General Data Protection Regulation (GDPR), (EU) 2016/679	Database Directive, (EC) 1996/9	Regulation for a Cybersecurity Act, (EU) 2019/881	Law Enforcement Directive, (EU) 2016/680	Product Liability Directive (PLD), (EEC) 1985/374, 2022/0302(COD)	Unfair Contract Terms Directive (UCTD), (EEC) 1993/13	Technology Transfer Block Exemption, (EC) 2014/316	Satellite and Cable I Directive, (EEC) 1993/83
InvestEU Programme Regulation, (EU) 2021/523	Radio Spectrum Decision, (EC) 2002/676	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1725	Community Design Directive, (EC) 2002/6, 2022/0391(COD)	Regulation to establish a European Cybersecurity Competence Centre, (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment, (EU) 2019/713	European Standardization Regulation, (EU) 2012/1025	E-commerce Directive, (EC) 2000/31	Company Law Directive, 2023/0083(COD)	Information Society Directive, (EC) 2001/29
Connecting Europe Facility Regulation, (EU) 2021/11153	Broadband Cost Reduction Directive, (EU) 2014/61, 2023/0046(COD)	Regulation on the free flow of non-personal data, (EU) 2018/1807	Enforcement Directive (IPR), (EC) 2004/48	NIS 2 Directive, (EU) 2022/2555	Regulation on terrorist content online, (EU) 2021/784	Radio Equipment Directive (RED), (EU) 2014/53	Unfair Commercial Practices Directive (UCPD), (EC) 2005/29	Market Surveillance Regulation, (EU) 2019/1020	Audio-visual Media Services Directive (AVMSD), (EU) 2010/13
Regulation on High Performance Computing Joint Undertaking, (EU) 2021/1173	Open Internet Access Regulation, (EU) 2015/2120	Open Data Directive (PSI), (EU) 2019/1024	Directive on the protection of trade secrets, (EU) 2016/943	Information Security Regulation, 2022/0084(COD)	Temporary CSAM Regulation, (EU) 2021/1232, 2022/0155(COD)	eiDAS Regulation, (EU) 2014/910, 2021/0136(COD)	Directive on Consumer Rights (CRD), (EU) 2011/83	P2B Regulation, (EU) 2019/1150	Portability Regulation, (EU) 2017/1128
Regulation on Joint Undertakings under Horizon Europe, (EU) 2021/2085, 2022/0033(INI, E)	European Electronic Communications Code Directive (EECC), (EU) 2018/1972	Data Governance Act (DGA Regulation), (EU) 2022/668	Standard essential patents, 2023/0133(COD)	Cybersecurity Regulation, 2022/0085(COD)	E-evidence Regulation, 2018/0108(COD)	Regulation for a Single Digital Gateway, (EU) 2018/1724	e-invoicing Directive, (EU) 2014/55	Vertical Block Exemption Regulation (VBER), (EU) 2022/720	Satellite and Cable II Directive, (EU) 2019/789
Decision on a path to the Digital Decade, (EU) 2022/2481	Roaming Regulation, (EU) 2022/612	ePrivacy Regulation, 2017/0003(COD)	Design Directive, 2022/0392(COD)	Cyber Resilience Act, 2022/0272(COD)		General Product Safety Regulation, (EU) 2023/988	Geo-Blocking Regulation, (EU) 2018/302	Digital Market Act (DMA Regulation), (EU) 2022/1925	Copyright Directive, (EU) 2019/790
European Chips Act (Regulation), 2022/0032(COD)	Regulation on the Union Secure Connectivity Programme, (EU) 2023/588	European Data Act (Regulation), 2022/0047(COD)	Compulsory licensing of patents, 2023/0129(COD)	Cyber Solidarity Act (Regulation), 2023/0109(COD)		Machinery Regulation, (EU) 2023/1230	Digital content Directive, (EU) 2019/770	Regulation on distortive foreign subsidies, (EU) 2022/2560	European Media Freedom Act, 2022/0277(COD)
European critical raw materials act (Regulation), 2023/0079(COD)	.eu top-level domain Regulation, (EU) 2019/517	European Health Data Space (Regulation), 2022/0140(COD)				AI Act (Regulation), 2021/0106(COD)	Directive on certain aspects concerning contracts for the sale of goods, (EU) 2019/771	Horizontal Block Exemption Regulations (HBER), (EU) 2023/1066, (EU) 2023/1067	
Establishing the Strategic Technologies for Europe Platform (STEP), 2023/0199(COD)		Regulation on data collection for short-term rental, 2022/0358(COD)				Eco-design Regulation, 2022/0095(COD)	Digital Services Act (DSA Regulation), (EU) 2022/2065	Platform Work Directive, 2021/0414(COD)	
		Harmonization of GDPR enforcement 2023/0202(COD)				AI Liability Directive, 2022/0303(COD)	Right to repair Directive, 2023/0083(COD)	Single Market Emergency Instrument (SMEI), 2022/0278(COD)	
		Interoperable Europe Act, 2022/0379(COD)					Political Advertising Regulation, 2021/0381(COD)		

Table 2: Overview of EU Enforcement Mechanisms and Agencies in the Digital sector

Explanation	1 EU Institution	2 Decentralised agency	3 Independent body	4 Network of Member States
	5 Executive agency	6 Governing board	7 Advisory body	8 European Standardisation Organisations

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-Commerce & Consumer Protection	Competition	Media	Finance
1 European Commission (DG DEFIS) Unit B.1 (EUJ 2021/694, EUJ 2021/695)	1 European Commission (DG JUST) Unit B.1 (EUJ 2023/588)	5 Body of European Regulators for Electronic Communications (BEREC) (EUJ 2018/1072)	1 European Health Data Space Board (EHDSB) (2022/01406/COD)	2 European Union Intellectual Property Office (EUIPO) (EUJ No.386/2012, EUJ 2017/1001, 2022/0391/COD, 2022/0392/COD, 2023/01298/COD, 2023/01330/COD)	1 cert-eu (2022/00866/COD)	2 Europol (EUJ 2016/794)	6 European Artificial Intelligence Board (2021/01066/COD)	1 European Commission (DG JUST) Unit B.3 (Consumer Enforcement and Redress)	1 European Commission (DG CNCT) Unit F.2 & F.3 (EUJ 2022/2085, EUJ 2022/1925)	1 European Regulators Group for Audiovisual Media Services (ERGA), potentially replaced by European Board for Media Services, (2021/6462, EUJ 2019/113, 2022/0273/COD)	1 European Central Bank (ECB) (EUJ 2015/2366, 2023/0212/COD)
2 European Research Council Executive Agency (ERCEA) (EUJ 2021/694, EUJ 2021/695, EUJ 2021/1773)	2 European Union Agency for the Space Programme (EUSPA) (EUJ 2023/588, EUJ 2021/696)	4 Interoperable Europe Board (2022/03786/COD)	4 European Data Protection Board (EDPB) (EUJ 2018/678)	1 European Patent Organization	5 European Cybersecurity Competence Centre (ECCC) (EUJ 2021/687)	2 Eurolat (EUJ 2018/1727)	5 Gateway coordination group (EUJ 2017/1724)	7 Consumer Protection Cooperation Network (EPCN) (EUJ 2017/2394)	1 European Commission (DG COMP)		1 European Securities and Markets Authority (ESMA) (EUJ 2022/2554, EUJ 2023/1114)
2 European Innovation Council & SMEs Executive Agency (EISMEA) (EUJ 2021/694, EUJ 2021/695, EUJ 2021/1773)	4 European Chips Infrastructure Consortium (EICIC) (2022/00303/COD)	4 eu Multistakeholder (EUJ 2018/117)	4 European Data Protection Supervisor (EDPS) (EUJ 2018/1725)	4 Compulsory licences advisory body (2023/01298/COD)	5 EU Agency for Cybersecurity (ENISA) (EUJ 2013/981)	2 European Public Prosecutor's Office (EPPO) (EUJ 2017/1939)	1 European Committee for Standardization (CEN) (EUJ 2012/1024)	1 Consumer Safety Network (EUJ 2023/988)	1 European Commission (DG GROW) Unit A.4 (2022/0278/COD)		5 European Banking Authority (EBA) (EUJ 2015/2366, EUJ 2022/2554, EUJ 2023/1114, 2023/0205/COD)
2 European Research Executive Agency (REA) (EUJ 2021/694, EUJ 2021/695, EUJ 2021/1773)	4 "Governing Board of Chips Joint Undertaking (Chips JU) (2022/03303/COD)"	4 Governing Board of Smart Networks and Services Joint Undertaking (SNS JU) (EUJ 2021/2065)	4 European Data Innovation Board (EDIB) (EUJ 2022/868)	4 European Observatory on Infringements of IPR (EUJ 386/2012)	3 European Defence Agency (EDA) (EUJ 2019/981)	2 Frontex (EUJ 2019/1896)	3 European Committee for Electrotechnical Standardization (CENELEC) (EUJ 2012/1025)		4 European Board of Digital Services (EUJ 2022/2065)		5 European Insurance and Occupational Pensions Authority (EIOPA) (EUJ 2022/2554, 2023/0205/COD)
4 European Institute of Innovation & Technology (EIT) (EUJ 2021/694, EUJ 2021/695, EUJ 2021/1773)	4 Governing Board of European High-Performance Computing Joint Undertaking (EuroHPC JU) (EUJ 2021/1773)				4 European Cyber Shield (2023/01096/COD)	2 eu-LISA (EUJ 2018/1738)	3 European Telecommunications Standards Institute (ETSI) (EUJ 2012/1026)		4 High-Level Group on DMA (EUJ 2022/1925)		
	4 European Digital Infrastructure Consortium (EDIC) (EUJ 2022/2461)				5 European Cybersecurity Certification Group (ECCG) (EUJ 2019/981)	2 EU Fundamental Rights Agency (FRA) (ECJ No.168/2007)			7 European Competition Network (ECN)		
	4 European Space Agency (ESA) (EUJ 2023/588)				4 Interinstitutional Cybersecurity Board (ICB) (2022/00866/COD)	5 European Anti-Fraud Office (1999/352/EC)			5 Union Product Compliance Network, (EUJ 2019/1026)		
	4 European Semiconductor Board (2022/00303/COD)				4 Interinstitutional Information Security Coordination group (2022/00866/COD)						
	4 European Critical Raw Materials Board (2023/00786/COD)				5 NIS cooperation group (EUJ 2022/2555)						
	7 European network of competence centres in semiconductors (2022/00303/COD)				2 Network of National Coordination Centres (EUJ 2021/987)						
					7 EU Cybersecurity Reserve (2023/01096/COD)						

Ma prendiamo i **Fantastici 4**
Le principali norme che tutti
bene o male conosciamo:

IA ACT, NIS2, CRA e GDPR



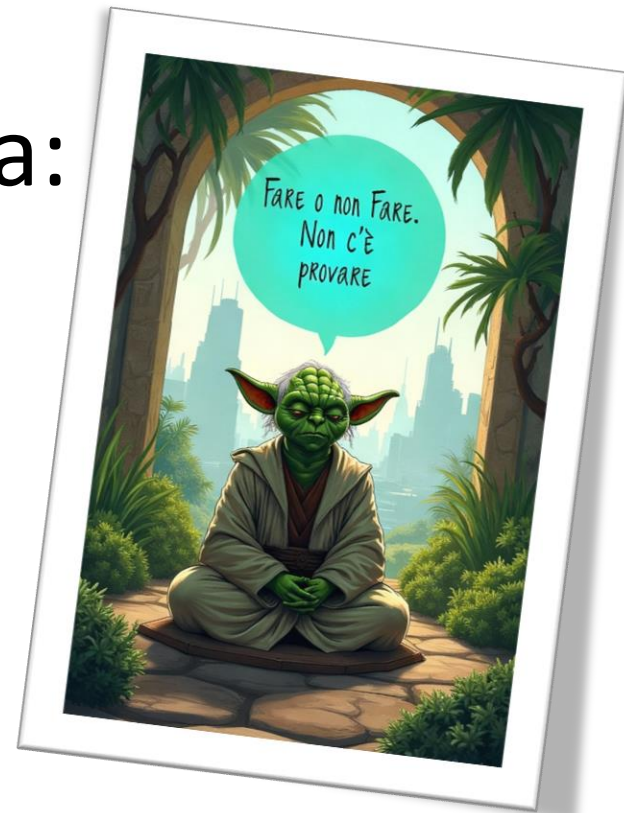
Immagine dalla copertina di
Noi siamo i Fantastici Quattro. Ediz. 60 anni

Tutti siamo «fornitori» di qualcuno.

E questi qualcuno,
spesso, sono soggetti
impattati dalle varie
norme.



Parafrasando il maestro Yoda:
Serve farlo.
Non provare.
Non immaginarlo.
E serve metterlo in pratica.



Conoscere è potere



Analizzare & Suddividere Ecco la risposta

Valutare le vulnerabilità

Individuare, analizzare e correggere i punti deboli prima che vengano sfruttati

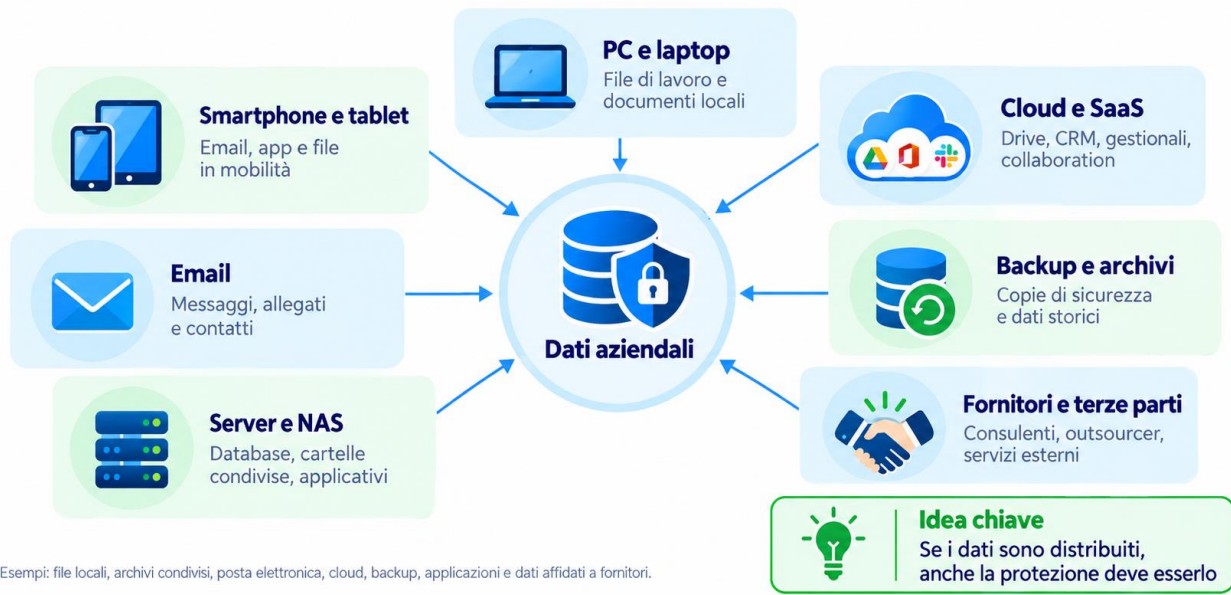


Esempi: software non aggiornato, configurazioni errate, password deboli, servizi esposti

1 Dove sono i dati

Dove sono i dati aziendali?

I dati di un'azienda non si trovano in un solo punto: sono distribuiti tra persone, dispositivi, sistemi e servizi.



2

La politica degli accessi



3

Ridurre La superficie d'attacco

Ridurre la superficie di attacco

Limitare i punti esposti per diminuire le opportunità di attacco e migliorare la sicurezza



Esempi: rimuovere software non usato, disattivare account inutilizzati, chiudere porte aperte, scollegare dispositivi non gestiti.

4 Misure di sicurezza



5

Procedure & Piani

Procedure e piani

In cybersecurity, vanno gestiti come un ecosistema coordinato tra norme, processi e controlli



Esempi: piano incidenti, gestione vulnerabilità, continuità operativa, DPIA, procedure IA, notifiche e registri.

5

Procedure & Piani

Procedure e piani

In cybersecurity, vanno gestiti come un ecosistema coordinato tra norme, processi e controlli



Esempi: piano incidenti, gestione vulnerabilità, continuità operativa, DPIA, procedure IA, notifiche e registri.



Grazie per l'attenzione

Fabio Zanolì

DPO, cybersecurity expert, docente.

*Referente per la regione EMILIA-ROMAGNA di ASSO
DPO*

info@nwnsolutions.it

NWN solutions - Bologna

Cybersecurity - GDPR Compliance - Web

<https://nwn.solutions>