NIS-2 & GDPR

Two regimes, one security goal — how they interact, overlap and reinforce each other

Field Talk – November 18th, 2026 – www.fieldtalk.eu

By : Koen Hostyn – Privacy for All

TOPICS

1. Regulation vs. Directive — the structural difference
2. Scope of application — who is caught by both regimes
3. Breach notification — parallel obligations and timelines
4. Supplier & vendor management
5. Security requirements & Article 32 GDPR
6. CyberFundamentals (CyFun) as an example model for "adequate measures"
7. Key requirements per CyFun level (Basic / Important / Essential)
8. Enforcement: why falling short might hit you twice

1. REGULATION VS. DIRECTIVE

GDPR: A REGULATION

- **Regulation (EU) 2016/679** — directly applicable in all Member States
- No transposition needed: **uniform, identical obligations** across the EU (with limited *openings* for national law, e.g. DPA powers, employment context)
- Applies to every controller and processor of personal data, regardless of size or sector
- Enforcement: national supervisory authorities + EDPB coordination

Legal nature: a Regulation is *directly effective law* on day one.

NIS-2: A DIRECTIVE

- **Directive (EU) 2022/2555** — must be **transposed** into national law
- Transposition deadline: 17 October 2024
- **Belgium:** Wet van 26 april 2024 + Koninklijk Besluit van 9 juni 2024 — in force since **18 October 2024**
- Member States keep **discretion**: national definitions, competent authorities, sectoral authorities, sanctions regimes, registration duties
- Result: **27 national variants** of the same directive — always check local law

Consequence: GDPR obligations are (quasi) identical everywhere; NIS-2 duties take their final shape from each Member State's transposition act.

SIDE-BY-SIDE

	GDPR	NIS-2
Instrument	Regulation (directly applicable)	Directive (transposed nationally)
Scope	All processing of personal data	Essential & important entities in 18 sectors
Trigger	Personal data	Network & information systems / services
Supervision	Data protection Authority	Cyber Security Authority + sectoral authorities
Focus	Rights of individuals	Resilience of services & society

2. BREACH NOTIFICATION

TWO NOTIFICATION REGIMES, TWO CLOCKS

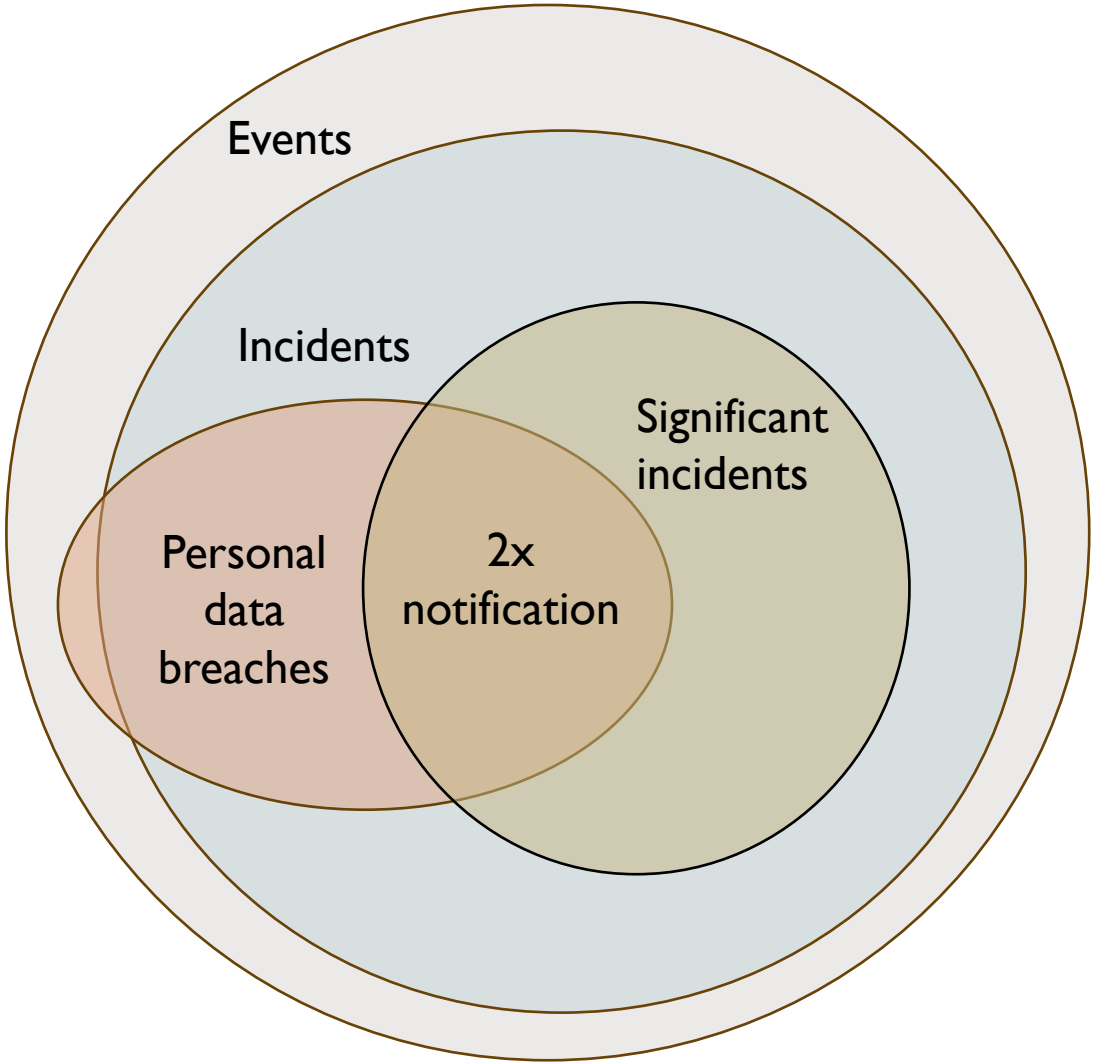
	GDPR Art. 33–34	NIS-2 Art. 23
What triggers it	**Personal data breach** (breach of security leading to loss of confidentiality, integrity or availability of personal data)	**Significant incident** (serious disruption of services / cyber impact)
Early warning	—	**Within 24 hours** of becoming aware
Main notification	**Within 72 hours** to the supervisory authority	**Within 72 hours** — initial incident notification
Follow-up	Possible updates	Intermediate report on request
Final report	—	**Within 1 month**
To whom	Data Protection Authorities (+ data subjects if high risk)	Cyber Security Authorities (+ affected in certain cases)

INTERPLAY IN PRACTICE

- **One incident, two regimes.** A ransomware attack that exfiltrates personal data is *both* a significant NIS-2 incident *and* a personal data breach.
- **Parallel notifications** are required — notifying the CSIRT does **not** discharge the GDPR duty, and vice versa.
- The **24h NIS-2 early warning** effectively pre-empts the GDPR 72h clock: prepare both notifications together.
- **Detection capability is a prerequisite:** you cannot notify what you cannot detect → logging, monitoring and incident processes serve both regimes (CyFun: OPS-04, INC-01).

Design **one incident process** with two notification tracks — never two separate playbooks.

INTERPLAY IN PRACTICE



3. SUPPLIER & VENDOR MANAGEMENT

NIS-2: SUPPLY CHAIN SECURITY IS A CORE DUTY

Art. 21(2)(d): cybersecurity risk-management measures must cover **the security of the supply chain, including security-related aspects of the relationships with each direct supplier or service provider**.

- Risk assessments of suppliers and their **sub-suppliers**
- Supplier incidents must be assessable (contractual duty to inform)
- Art. 21(3): essential entities must consider **supply-chain specific risks** at advanced level
- Focus on: cloud providers, MSPs, software vendors, critical dependencies

GDPR: THE PROCESSOR REGIME

- **Art. 28:** use only processors with **sufficient guarantees**; written contract with mandatory clauses (instructions, confidentiality, security, sub-processors, assistance, deletion/return, audits)
- **Art. 32 applies directly to processors** — vendors processing personal data carry their own security duty
- **Art. 28(3)(h):** audit & inspection rights must be contractually secured
- **Chapter V:** transfers outside the EU need an additional legal mechanism (adequacy, SCCs)
- **Art. 24 & 5(2) accountability:** the controller remains responsible for choosing and overseeing vendors

ONE VENDOR FRAMEWORK, BOTH REGIMES

Overlapping requirements — build once, use twice:

- Vendor risk assessment at onboarding + periodic reassessment
- Security clauses in contracts (incident notification, audit rights, sub-processing)
- Inventory of suppliers and the data/systems they touch
- Monitoring and exit strategies
- Due diligence evidence (e.g. CyFun label or ISO 27001 certificate of the vendor)

A **CyFun label or ISO 27001 certificate** of a supplier can serve as practical evidence of "sufficient guarantees" under Art. 28 GDPR *and* of supply-chain risk management under Art. 21(2)(d) NIS-2

4. SECURITY REQUIREMENTS & ARTICLE 32 GDPR

NIS-2 ART. 21: THE MINIMUM MEASURE SET

Risk-management measures appropriate to the entity's risk, including **all-hazards** approach covering at least:

1. **Risk analysis** & information-system security policies
2. **Incident** handling
3. **Business continuity**, backup, disaster recovery & crisis management
4. **Supply-chain security** (incl. relationships with direct suppliers)
5. Security in **acquisition**, development & maintenance, incl. vulnerability handling
6. Policies to **assess effectiveness** of the measures
7. **Cyber hygiene & training**
8. **Cryptography & encryption**
9. **HR security**, access control & asset management
10. **Multi-factor authentication** & secured communications

GDPR ART. 32: "APPROPRIATE TECHNICAL AND ORGANISATIONAL MEASURES"

Taking into account **the state of the art, costs of implementation, and the nature, scope, context and purposes of processing, as well as the risk**:

- Pseudonymisation & **encryption**
- Ongoing **confidentiality, integrity, availability and resilience** of processing systems
- Ability to **restore availability and access** to personal data in a timely manner (backups)
- **Process for regularly testing, assessing and evaluating** the effectiveness of the measures

Art. 5(1)(f): integrity and confidentiality as a principle of processing. **Art. 5(2):** accountability — the controller must be able to *demonstrate* compliance.

5. CYBERFUNDAMENTALS (CYFUN) —AN EXAMPLE MODEL FOR "ADEQUATE MEASURES"

WHAT IS CYFUN? (CYFUN.EU)

- Belgium's **national cybersecurity framework**, maintained by the **Centre for Cybersecurity Belgium (CCB)**
- Co-scheme owners: **Belgium, Ireland and Romania** — moving toward EU mutual recognition
- In Belgium, NIS-2 entities must adopt **CyFun or ISO 27001** (and thus map CyFun requirements to ISO annex A controls)
- Built on **NIST CSF 2.0**, ISO/IEC 27001–27002, CIS Controls and IEC 62443 (OT)
- CyFun 2025: **6 functions, 22 categories, 106 subcategories**, incl. a dedicated **Governance** function
- **Cumulative assurance levels** (Small, Basic, Important, Essential) with an official **verification/certification scheme**

RISK-BASED APPROACH

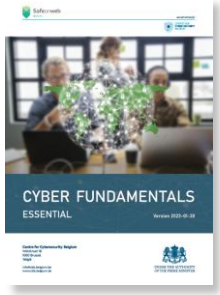
CENTRE FOR CYBERSECURITY BELGIUM

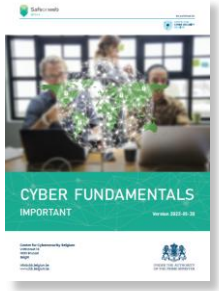
Version: 2023-08-03

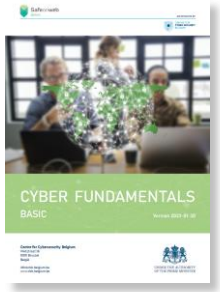
Energy			*Common skills*		*Common skills*		*Common skills*		*Extended Skills*		*Extended Skills*			
Organization Size (L/M/S = 3/2/1)	**3**	*Threat Actor Type*	**Competitors**		**Ideologues Hactivists**		**Terrorist**		**Cyber Criminals**		**Nation State actor**			
Cyber Attack Category	*Global or Targetted*	*Impact*	*Prob*	*Risk Score*	*Prob*	*Risk Score*	*Prob*	*Risk Score*	*Prob*	*Risk Score*	*Prob*	*Risk Score*		
Sabotage/ Disruption (DDOS,...)	2	High	Low	0	Low	0	Med	30	Med	30	High	60		
Information Theft (espionage, ...)	2	High	Low	0	Low	0	Low	0	High	60	High	60		
Crime (Ransom attacks)	1	High	Low	0	Low	0	Low	0	High	30	Low	0		
Hactivism (Subversion, defacement...)	1	Med	Low	0	Med	7,5	Low	0	Low	0	Med	7,5		
Disinformation (political influencing)	1	Low	Low	0	Med	0	Low	0	Low	0	Low	0	Score	CyFun Level
	Total	Total		0		7,5		30		120		127,5	**285**	**ESSENTIAL**

Essential entities

Important entities







THE THREE CUMULATIVE LEVELS

Level	Controls	Key Measures	Target
Small (2023)	10 controls	/	Micro-organisations without IT department
Basic	34 controls	13 key measures	Entry-level security hygiene
Important	133 controls	22 key measures	Higher-risk & important entities
Essential	218 controls	29 key measures	Essential (NIS-2) entities

BASIC— SECURITY HYGIENE

For all organisations — the "floor" for any organisation holding personal data

- **Password policy & multi-factor authentication** (MFA on remote access, admin & internet-facing accounts)
- **Patch management** — timely security updates for systems and software
- **Malware protection** (antivirus/EDR) on endpoints
- **Backups** — regular, tested, incl. offline copies
- **Asset inventory** & network protection (firewall, secure Wi-Fi)
- **Logging of security events**
- **Encryption** of sensitive data at rest & in transit
- **Phishing & awareness training** for staff
- **Mobile device & cloud usage policy**
- **Email and browser hardening**

Covers > 80% of the attack vectors seen by CSIRT.be (CCB incident statistics).

IMPORTANT— MANAGED SECURITY

Expected of larger organisations and NIS-2 "important" entities

- **Formal risk assessments** & security policy framework
- **Incident management process** (detection, escalation, lessons learned)
- **Supplier & supply-chain management** — due diligence, security clauses, monitoring (SUP-01 → SUP-04)
- **Secure development** practices & vulnerability management lifecycle
- **Network segmentation** & internal firewalls; hardening of remote access (VPN)
- **Identity & privileged access management** (separate admin accounts, session logging)
- **Centralised logging (SIEM)**, correlation & retention (12+ months)
- **Physical security & HR security** (onboarding/offboarding, screening)
- **Business continuity & disaster recovery plans** with defined RTO/RPO

ESSENTIAL— ADVANCED & PROACTIVE

Expected of NIS-2 "essential" entities — highest assurance

- **24/7 security monitoring** (SOC / managed detection & response)
- **Advanced threat detection & threat intelligence** integration
- **Penetration testing & red teaming** on a recurring schedule
- **Advanced cryptography management** (key management, HSM, crypto-agility)
- **Resilience & redundancy** — high availability, immutable/offline backups, DR testing (tabletop → full restoration)
- **OT security** (IEC 62443 alignment) where industrial systems are in scope
- **Mature security governance**: risk committee, internal audit, continuous improvement, KPI reporting to management
- **Supply-chain assurance** at advanced level (sub-supplier risk, contractual enforcement)

The 13 CyFun 2025 "Key Measures" (MFA, offline backups, patching, segmentation, EDR, PAM, awareness, SIEM, IR plan, asset inventory, supply chain, encryption, continuity) cut across all levels and are the CCB's stated priorities.

WHY CYFUN IS A MODEL FOR ART. 32 GDPR

GDPR Art. 32 requires measures "appropriate to the risk" and reflects **"the state of the art"**. CyFun operationalises exactly that:

- ✅ **Risk-based & proportionate** — levels scale with the entity's profile
- ✅ **State of the art** — derived from NIST CSF 2.0 / ISO 27001, the internationally recognised benchmark
- ✅ **Measurable & auditable** — control-by-control maturity scoring (documentation + implementation)
- ✅ **Independently verified** — accredited Conformity Assessment Bodies (BELAC) issue an official label
- ✅ **Covers the personal-data-relevant controls:** encryption, access control, logging, backup, incident respons

A CyFun assessment report is **strong, contemporaneous evidence** that an organisation took "adequate technical and organisational measures" — the exact phrase used in GDPR Art. 32 and Art. 34(3)(a) (breach safeguards).

Enforcement 2018–2026

—

what authorities actually penalise

ART. 32 IN PRACTICE

Year	Authority	Entity	Fine	Security measures lacking
2018	**LfDI Baden-Württemberg** (DE)	Knuddels.de (chat platform)	€20k	Passwords stored in **plaintext** (unhashed) — no pseudonymisation/encryption; first GDPR fine in Germany (Art. 32(1)(a))
2019	**CNIL** (FR)	SERGIC (real estate)	€400k	Rental applicants' supporting **documents accessible on the website** without adequate security; unlimited retention (Art. 32 + 5(1)(e))
2019	**AP** (NL)	HagaZiekenhuis (hospital)	€460k (reduced to €350k on appeal, 2021)	Insufficient internal security of patient records — staff accounts without **two-factor authentication** (Art. 32)
2019	**BfDI** (DE)	1&1 Telecom (telco)	€9.55M	Telephone customer service: callers identified via easily researched knowledge — inadequate technical & organisational measures (Art. 32)
2020	**ICO** (UK)	British Airways	£20M (NOI £183.4M)	Magecart skimming, 429,612 data subjects: **no MFA, insufficient network segmentation**, untested payment-page security (Art. 5(1)(f), 32)
2020	**ICO** (UK)	Marriott	£18.4M (NOI £99.2M)	Starwood breach, up to 339M records: **no privileged-account monitoring**, **no MFA** on database, **unencrypted passports**; compromise undetected for 4 years (Art. 5(1)(f), 32)
2021	**GBA/APD** (BE)	Financial institution	€100k	Shared password for manager access to the Central Credit Register — no individual **access control**, **no logging**: "blatant violation" of Art. 32 (also Art. 25, 5(2))

ART. 32 ENFORCEMENT 2018–2021 — EXAMPLE DECISIONS

Year	Authority	Entity	Fine	Security measures lacking
2024	**DPC** (IE)	Meta Platforms Ireland	€91M	Passwords stored in **plaintext**, readable by staff — no encryption or pseudonymisation (Art. 32(1)(a))
2024	**UODO** (PL)	Medical company (hacking incident)	€330k	Insufficient technical & organisational measures following a hacker attack (Art. 5(1)(f), 24, 32)
2024	**UODO** (PL)	Door-seller company (+ its processor's partners fined PLN 9.8k)	€81k	Ransomware via employee-disabled antivirus & unpatched server: **no risk analysis**, failure to verify the processor's guarantees, defective breach notification (Art. 5(2), 24, 25, 32)
2025	**ICO** (UK)	Advanced (NHS software processor)	£3.07M	Ransomware entered via customer account **without MFA**; processor's own security duty; late breach notification (Art. 32(2), 33(2))
2026	**CNIL** (FR)	Free Mobile & Free	€42M	24M records incl. IBANs: **VPN remote access without adequate authentication**, ineffective anomaly detection; faulty breach notice (Art. 32, 34, 5(1)(e))
2026	**Garante** (IT)	WINDTRE	€1.7M	Two **social-engineering breaches**, 365k customers: "serious data security shortcomings" (Art. 32)
2026	**Garante** (IT)	Engineering consultancy	€120k	Ransomware via **VPN without second factor**; Garante published a checklist of "common-use" measures (Art. 5(1)(f), 32)
2026	**ICO** (UK)	South Staffordshire Water	£963.9k	Phishing-led intrusion (Sep 2020), attacker took admin rights; minimal monitoring, obsolete systems, no regular security scans — **undetected for 20 months** (Art. 5(1)(f), 32(1))

ART. 32 ENFORCEMENT 2022–2026 — THE MESSAGE GETS SHARPER

WHAT ART. 32 AUTHORITIES CONSISTENTLY PENALISE

- **MFA on remote access & privileged accounts** — BA, Advanced, Free, Garante 2026 cases → CyFun key measure #1 (ACC-03)
- **Logging, monitoring & detection capability** — GBA 2021, Marriott, Free, South Staffordshire → SIEM/EDR, logging controls (OPS-04)
- **Encryption & password hygiene** — Knuddels, Meta, Marriott → CRY domain, key measure #12
- **Patching & system currency** — Free, South Staffordshire, UODO door-seller case → key measure #3 (OPS-03)
- **Processors carry their own Art. 32 duty** — Advanced (£3.07M, fined directly as processor); in Poland the vendor's partners were fined for the unpatched server, and the controller for failing to verify it (UODO 2024)
- **Burden of proof on the controller** — being the victim of a crime is *no defence*: the Garante (2026) held the ransomware breach "neither unforeseeable nor inevitable" and that **"common-use" measures would have prevented it**

The recurring catalogue of deficiencies can be mapped to **the CyFun Basic key-measures list**. Regulators are, in effect, already applying a CyFun-style "state of the art" benchmark.

7. ENFORCEMENT: FALLING SHORT HITS YOU TWICE

DOUBLE ENFORCEMENT

- Fines can be **cumulative** — the GBA and the CCB are independent enforcers
- **Reputational amplifier:** breach notification + public enforcement + client audits
- **EDPB/GBA case law**: attackers exploited *exactly* the controls CyFun Basic mandates → inadequate Art. 32 measures

SANCTIONS — STACKED, NOT ALTERNATIVE

	GDPR	NIS-2 (Belgium)
Art. 5 (principles)	Up to **€20 M or 4%** global turnover	—
Art. 32 (security)	Up to **€10 M or 2%**	Essential entities: up to **€10 M or 2%**
Other tier	Art. 33/34 up to €10 M / 2%	Important entities: up to **€7 M or 1.4%**
Management	—	**Personal liability** (Art. 20): formal notice, training orders, temporary ban
Extra	Data-subject claims, DPA audits & corrective orders	Enforcement powers: audits, binding instructions, certification duties

FAILURE TO MEET THE STANDARD = DOUBLE EXPOSURE

Argument: if an organisation subject to both regimes fails to implement its applicable CyFun level (or equivalent ISO 27001), that same gap is *simultaneously*:

- a **NIS-2 non-compliance** (Art. 21 risk-management measures not met, as concretised by the Belgian law's CyFun/ISO obligation), **and**
- a **GDPR violation**:
  - **Art. 5(1)(f)** — breach of the integrity & confidentiality principle
  - **Art. 5(2)** — failure to *demonstrate* accountability (no evidence of adequate measures)
  - **Art. 32** — "appropriate technical and organisational measures" not in place

Important to note : this could also **apply also to non-NIS-2 entities** since CyFun Basic is to be considered 'basic cyber hygiene' by all companies

- Applies especially those in the **supply chain** of NIS-2 entities
- **Main difference** : non-NIS-2 entities are not liable for NIS-2 fines and ex-ante or ex-post controls by cyber security authorities

WHY THE ARGUMENT HOLDS

1. **The control set is the same.** Missing MFA, no offline backups, no patching → inadequate measures *under both* Art. 21 NIS-2 *and* Art. 32 GDPR. One deficiency, two violations.
2. **"State of the art" is externally defined.** CyFun is an official benchmark — a supervisory authority or court can treat non-attainment as strong evidence that measures fell below the state of the art.
3. **Absence of evidence is evidence.** Art. 5(2) GDPR requires demonstrable compliance. No CyFun self-assessment, no certification, no audit trail → accountability failure in its own right.
4. **Incidents connect the dots.** A preventable breach (e.g. unpatched system, phished account without MFA) proves the inadequacy retrospectively — triggering both NIS-2 enforcement *and* GDPR Art. 33/34 procedures.

CONCLUSION: ONE CONTROL FRAMEWORK, TWO OBLIGATIONS

PRACTICAL TAKE-AWAYS

1. **Transposed ≠ uniform.** GDPR duties are identical EU-wide; NIS-2 duties depend on the Belgian law & royal decree — map both.
2. **One incident process, two notification tracks** (24h/72h/1 month vs 72h) — detect once, possibly notify twice.
3. **One vendor governance programme** covering Art. 21(2)(d) NIS-2 and Art. 28 GDPR.
4. **Adopt CyFun (or similar) as the backbone:** it satisfies the NIS-2 obligation *and* provides demonstrable, state-of-the-art evidence for Art. 32 GDPR.
5. **Match your level to your profile** — Basic / Important / Essential
6. **Document everything:** evidence culture is the cheapest insurance against double fines.

SOURCES

Regulatory framework

- Directive (EU) 2022/2555 (NIS-2), Arts. 20–23, 32–34
- Regulation (EU) 2016/679 (GDPR), Arts. 5, 24, 28, 32–34, 83
- CyberFundamentals framework — CCB, cyfun.eu — CyFun 2025 booklets (Basic / Important / Essential), Key Measures, Conformity Assessment Scheme
- CCB Safeonweb@work — De NIS2-wet and the NIS-2 brochure

Art. 32 case law (2018–2026)

- **ICO:** Advanced £3.07m (+ CMS); BA £20m (TechCrunch + Bird & Bird); Marriott £18.4m (HSF + Lexology); South Staffordshire £963,900 (BBC + ICO notice)
- **DPC:** Meta €91m, plaintext passwords (DPC + BBC)
- **CNIL:** Free Mobile & Free €42m (CNIL délib. SAN-2026-001/002 + Delsol/Village-Justice); SERGIC €400k (CNIL délib. 28.05.2019 + TAoMA/AvocatsPi)
- **Germany:** LfDI BW — Knuddels €20k (LfDI press release + Dr. Bahr); BfDI — 1&1 Telecom €9.55m (BfDI + Der Spiegel)
- **Netherlands:** AP — HagaZiekenhuis (AP documents + Verzekeraars.nl; reduction on appeal per AP, 2021)
- **Poland:** UODO — medical company €330k (EDPB + Enforcement Tracker); UODO — door-seller €81k (UODO announcement + EDPB)
- **Belgium:** GDPRhub APD/GBA 56/2021 — €100k (GDPRhub + DataGuidance/NautaDutilh)
- **Italy:** WINDTRE €1.7m (Garante newsletter + Help Net Security); consultancy €120k, provvedimento n. 529/2026 (01magazine + Cybersecurity News)
- **Databases:** GDPR Enforcement Tracker, Wikipedia: GDPR fines and notices

Educational material — not legal advice. Verify scope, level and deadlines with your cyber securitu authority and your DPO/legal counsel.