GDPR security: could you prove your measures fit the risk?

This quarter, require MFA on every remote, partner and admin login, and link each entry in your Article 30 records to the systems, processors and measures that protect it. Judge every other measure by the harm a breach would do to the people concerned and by what the state of the art offers, because in a damages claim you must prove your measures were appropriate[3].

Reviewed	Next review	Version	Written for	Latest version
5 Nov 2026	**5 Dec 2026**	**1.1**	**IT, security and data protection teams in companies in Germany and the EU**	**sheets.einblick.dev/gdpr-security/**

If you only do five things

1. **Require MFA for every remote, partner and admin login.** Nearly 80% of the large breaches the CNIL saw in 2024 used a hijacked account protected only by a password, and from 2026 it checks large databases for MFA[10]. See the passkeys-mfa sheet.
2. **Link your records of processing to your asset list.** Give each Article 30 entry its systems and processors, next to the description of measures the GDPR asks for where possible[1], so no system goes live without an owner and a risk rating.
3. **Make processor contracts specific.** Attach a concrete security annex[18] with a regular review, and no changes that lower security without your approval[19].
4. **Patch known flaws and watch for bulk data access.** Patch within the patching sheet's deadlines. For large databases the CNIL expects alerts and caps on bulk exports[10].
5. **Clear monitoring tools with the works council first.** In Germany, the works council co-determines any system that records individualizable behavior or performance data, whatever you intend[6]. DLP that builds staff profiles also needs a DPIA[27].

Show that your measures fit the risk

1. **Which systems process the data?** Start from the Article 30 record. SDM 3.1a asks you to show that each means of processing, especially technical ones, is used lawfully[24].
2. **How much harm could a breach do?** Rate the risk for the people concerned, not for the company. Where your IT-Grundschutz rating differs, the SDM says to use the higher one or work out why they differ[23]. Likely high risk needs a DPIA first[1].
3. **What does the state of the art offer?** A moving target: what the market offers, as recognized standards show. Cost can shape the choice of measure but is no reason to skip one[21].
4. **Do the measures work?** Article 32 names encryption, pseudonymization, timely restore and regular testing[1]. Test restores, access rights and exposure on a schedule, and keep the results.
5. **Could you prove it in court?** A breach alone doesn't show your measures were inappropriate, but in a damages claim the burden of proof is yours[3].

What authorities fined for, 2024 to 2026

- **Weak remote logins.** The CNIL's €42 million fines on Free Mobile and Free in January 2026 cited weak VPN logins and ineffective detection of abnormal activity[11]. In September 2026 the CNIL announced a €500,000 fine on a private hospital: external doctors reached records without VPN or MFA, and the attacker browsed for days unnoticed[14].
- **Accounts that see too much.** France Travail's €5 million fine in January 2026 cited weak authentication, too little logging and partner advisers who could see jobseekers they didn't support[12].
- **Weak identity checks, unmonitored partners.** The BfDI fined Vodafone €45 million in June 2025: €30 million for portal and hotline authentication flaws that exposed eSIM profiles, €15 million for not monitoring partner agencies. Vodafone accepted and paid both[9].
- **Known flaws left open.** In October 2024, Italy's Garante announced a €900,000 fine on Postel for a flaw left unpatched for almost a year after the vendor and the national cyber agency flagged it[15].
- **No log review, no MFA.** IQVIA's €5 million fine in May 2026 included unreviewed connection logs and no MFA on a health data warehouse[13].
- **Secrets and design.** The Irish DPC fined Meta €91 million in 2024 for plaintext passwords[16] and €251 million after a flaw exposed access tokens, €240 million of it for failing data protection by design and default[17].

Processor contracts and the security annex

- **Describe measures concretely.** The standard clauses rule out generic descriptions[18]; the EDPB wants enough detail for you to judge them[19].
- **Know every subprocessor.** Keep each one's name, address and contact at hand; the processor should supply and update them[20]. Under a general authorization, you get notice of changes and a chance to object[1].
- **Scale checks to the risk.** Verify every processor, more deeply where the risk is higher[20]. For databases of millions of people, the CNIL expects the security policy and certification evidence annexed, and periodic audits[10].
- **See the other sheets.** Supplier tiers and exit terms are in third-party-risk, AI providers in ai-input-security.

Security monitoring and staff

- **Don't rely on § 26 BDSG alone.** The CJEU said a Hessian clause much like § 26(1) appears merely to restate the GDPR; a court that agrees must in principle disregard it[4]. Document an Article 6 basis per tool.
- **Agree each tool with the works council.** Under § 87(1) no. 6 BetrVG it co-determines systems that record individualizable behavior or performance data, with no threshold for minor tools[6]. Courts fully review whether a works agreement's processing is necessary[5].
- **Write a logging concept.** Per processing activity, state what is logged, where, why, who may read it and when it is deleted[25]; the CNIL suggests six months to a year for access logs[10]. Logs kept to check admin work must not be used to rate their speed[25].

How German authorities judge measures

- **The SDM is the yardstick.** It maps GDPR duties to seven goals[23], and the DSK recommends it with its catalog of reference measures[24].
- **Email needs enforced TLS.** For high risk, the DSK expects end-to-end and qualified transport encryption: TR-02102-2 ciphers, forward secrecy, DNSSEC-checked servers. Professional secrecy can signal high risk[26].
- **Check the DPIA must-list.** It names DLP that profiles staff, employee geolocation and AI that evaluates people or steers interaction with them[27].

What you can skip

- **End-to-end encryption for all email.** The DSK requires it only for high risk[26]. Enforce TLS for the rest.
- **A certificate to prove Article 32.** Approved certifications and codes of conduct are only one element of proof[1]. Spend on the controls.
- **Collecting every subprocessor contract.** The EDPB says you needn't ask for them systematically[20].
- **A DPIA for every system.** The Article 29 Working Party's rule of thumb is two of its nine criteria[22]. File a screening note for the rest.

What changed in 2026

- **The SDM logging module was rewritten.** Building block 43 v2.0, valid since 1 June 2026, asks for an organization-wide logging concept[25].
- **Fixed steps for cross-border cases.** For cases opened after 2 April 2027, you get preliminary findings and three to six weeks to reply[2].
- **Fewer firms may need records.** The Omnibus IV deal would exempt firms under 1,000 staff except for high-risk processing[28]; Parliament's indicative plenary date is 23 November 2026[29]. The Digital Omnibus is still a proposal[30].

Mistakes that cost the most

- **Naming measures and not building them.** The CNIL held it against France Travail that its DPIAs listed most of the missing measures[12].
- **Leaving processors out of scope.** A significant share of the large breaches the CNIL saw in 2024 involved a processor with weak security[10].
- **Sharing by default.** The BGH said open-by-default phone number search likely breached data minimization, and saw no objection to about €100 for the loss of control alone[7].
- **Dropping records under Omnibus IV.** High-risk processing would still need them[28], and without them you can't scope a breach.

What this looks like at your size

Small team, no security staff

- Keep records even with fewer than 250 staff: the exemption doesn't cover processing that isn't occasional, such as payroll[1].
- Turn on MFA for email, VPN and remote support tools first.
- File each provider's standard processing agreement with its security annex and subprocessor list.

Growing, with IT or security staff

- Make the Article 30 entry, risk rating and owner required fields when a system enters the asset list.
- Sign one framework works agreement for security tools that sets purposes, data, access, retention and the procedure on suspicion, as the BfDI advises for web logs[8].
- Keep a yearly test plan and its results as Article 32 evidence.

Enterprise or regulated

- Map SDM goals to your ISMS controls so one evidence set serves the GDPR, NIS2 and ISO 27001 (see the isms and eu-security-laws sheets).
- Audit high-risk processors and the subprocessors behind them on a schedule.
- Name who replies to preliminary findings in cross-border cases opened after 2 April 2027, possibly within three weeks[2].

Version history

5 Nov 2026, version 1.1 Stated Parliament's 23 November 2026 date for Omnibus IV as the indicative plenary date it is.

Sources

1. GDPR, Articles 28, 30, 32 and 35. EUR-Lex, 2016. eur-lex.europa.eu
2. Regulation (EU) 2025/2518. EUR-Lex, 12 Dec 2025. eur-lex.europa.eu
3. Judgment C-340/21. CJEU, 14 Dec 2023. eur-lex.europa.eu
4. Judgment C-34/21. CJEU, 30 Mar 2023. eur-lex.europa.eu
5. Judgment C-65/23. CJEU, 19 Dec 2024. eur-lex.europa.eu
6. Beschluss 1 ABN 36/18. BAG, 23 Oct 2018. bundesarbeitsgericht.de
7. Pressemitteilung 218/24. BGH, 18 Nov 2024. bundesgerichtshof.de
8. FAQ Beschäftigtendatenschutz. BfDI, checked 5 Nov 2026. bfdi.bund.de
9. BfDI imposes fines on Vodafone. BfDI, 3 Jun 2025. bfdi.bund.de
10. Sécurité des grandes bases de données. CNIL, 30 Apr 2025. cnil.fr
11. Sanction: Free Mobile et Free. CNIL, 14 Jan 2026. cnil.fr
12. Sanction: France Travail. CNIL, 29 Jan 2026. cnil.fr
13. Sanction: IQVIA. CNIL, 28 May 2026. cnil.fr
14. Sanction: Hôpital privé de la Loire. CNIL, 3 Sep 2026. cnil.fr
15. Newsletter n. 528 (Postel). Garante Privacy, 22 Oct 2024. garanteprivacy.it
16. DPC fines Meta €91 million. DPC Ireland, 27 Sep 2024. dataprotection.ie
17. DPC fines Meta €251 million. DPC Ireland, 17 Dec 2024. dataprotection.ie
18. Decision (EU) 2021/915, Annex III. EUR-Lex, 4 Jun 2021. eur-lex.europa.eu
19. Guidelines 07/2020, version 2.1. EDPB, 20 Sep 2022. edpb.europa.eu
20. Opinion 22/2024 on processors. EDPB, 7 Oct 2024. edpb.europa.eu
21. Guidelines 4/2019 on Article 25. EDPB, 20 Oct 2020. edpb.europa.eu
22. DPIA guidelines, WP248 rev.01. Article 29 WP, 4 Oct 2017. ec.europa.eu
23. SDM, Version 3.1a. DSK, 26 Feb 2025. datenschutz-mv.de
24. SDM und Bausteine. LfDI M-V, checked 5 Nov 2026. datenschutz-mv.de
25. SDM Baustein 43 Protokollieren, V2.0. DSK, 1 Jun 2026. datenschutz-mv.de
26. OH E-Mail. DSK, 16 Jun 2021. datenschutzkonferenz-online.de
27. DSFA-Muss-Liste, V1.1. DSK, 17 Oct 2018. datenschutzkonferenz-online.de
28. Omnibus IV provisional agreement, PE790.249. European Parliament, 26 Jun 2026. europarl.europa.eu
29. 2025/0130(COD), Omnibus IV. European Parliament, checked 5 Nov 2026. oeil.europarl.europa.eu
30. 2025/0360(COD), Digital Omnibus. European Parliament, checked 5 Nov 2026. oeil.europarl.europa.eu