

O3 GDPR and Safeguarding Data Handling

How to handle, store, share and protect safeguarding data in compliance with EU law

Purpose

This document provides GDPR-compliant guidance for handling safeguarding data — the personal and sensitive information that arises when safeguarding concerns are raised, recorded and managed.

EU member organisations: treat this as a complement to your existing GDPR policy. Non-EU organisations operating within Erasmus+ and ESC: GDPR applies to your processing of data about EU citizens. You are required to comply. This document covers the most important safeguarding-specific applications of GDPR principles.

1. What Safeguarding Data Is

Safeguarding data includes all personal information that arises in the context of safeguarding: the identity and contact details of the person at risk, the alleged perpetrator, witnesses and reporting parties; the content of disclosures; case records; investigation notes; monitoring plans; and case outcomes.

Safeguarding data is classified as special category data under GDPR Article 9 because it may concern: health and medical conditions; sexual orientation or sexual acts; criminal allegations; and information about children. Special category data requires a specific lawful basis and must be handled with heightened care.

2. Lawful Bases for Processing Safeguarding Data

Processing activity	
Recording a safeguarding concern and managing the response	GDPR Article 9(2)(b): processing necessary for obligations and rights in employment and social protection. Or Article 9(2)(c): vital interests — protecting the life or physical safety of the data subject or another person.
Sharing data with statutory authorities (police, social services)	Article 9(2)(c): vital interests. Or Article 9(2)(g): substantial public interest (child protection and safeguarding).
Sharing data across partner organisations or across national borders in an urgent case	Article 6(1)(d) and Article 9(2)(c): vital interests. Tell the person at risk what is being shared and why, before sharing where possible.
Retaining case records after case closure	Article 6(1)(c): legal obligation — statutory retention requirements vary by country. Minimum recommended retention: 6 years for adult cases; until the person reaches 25 for child cases. Check your national legal supplement.

Sharing anonymised data in the annual review (O4)	Article 6(1)(a): consent, or legitimate interests — data is anonymised and used for governance purposes only.
---	---

3. Who Can Access Safeguarding Data

Access to safeguarding data is restricted on a strict need-to-know basis. The following access levels apply:

Data type	
II Part A (Incident Form)	The DSL and Alternate DSL. In exceptional cases, the board chair or senior manager directly involved in case management.
II Part B (Case Log)	The DSL and Alternate DSL. External safeguarding advisor when engaged on the case.
II Part C (Identity Index — links codes to real names)	The DSL and Alternate DSL only. This is the most restricted document in the safeguarding system. It must never be combined with Parts A or B.
Monitoring plan records	DSL, Alternate DSL, and any named contact person in the monitoring plan.
Annual review data (anonymised)	Board and senior management. All identifying information removed before sharing.

Applying RASCI to access control: the DSL is Responsible and Accountable for all safeguarding data. The Alternate DSL is Supportive. The board chair is Consulted only for Major cases and governance-level decisions. External safeguarding advisors are Informed only when directly engaged on a case. All others: no access.

4. Information Sharing — All Relevant Parties

Safeguarding reporting involves sharing information with a range of parties. All sharing must comply with the need-to-know principle and GDPR.

Party	
Person at risk	What information is being shared, with whom, and why — told before sharing where possible. Kept informed throughout the case. In most cases their consent is sought (not required, but good practice where it does not compromise safety).
Person who raised the concern	Confirmation that the concern was received and is being acted on. Not the full case details.
Alleged perpetrator	That a concern has been raised, at the appropriate point in the process (see I4 Section 3). General nature of the concern. Not the full disclosure details or the identity of the reporter. Not the full case log.

Parents, caregivers and legal guardians	Where the person at risk is a child or does not have capacity to consent: involved in the response as appropriate. Their contact details should be collected at the start of any project involving under-18s (R2 Consent Forms).
Partner organisations	Information shared on need-to-know basis. Only the partner's named safeguarding contact receives case information. Cross-border: vital interests basis applies.
Statutory authorities	Full disclosure as required for the referral. The DSL leads on this. Record what was shared, to whom and when.
Board and trustees	Anonymised summary data at annual review (O4). Major cases: informed promptly. Individual case details: only what is needed for governance decisions.

5. Storage and Security

- All safeguarding records stored in a password-protected, access-controlled system. Not on shared drives accessible to non-DSL staff.
- I1 Part C (Identity Index) stored in a separate, more restricted location from Parts A and B.
- Physical copies (printed incident forms, signed codes of conduct) stored in a locked cabinet accessible only to the DSL.
- No safeguarding information stored on personal devices, personal email accounts or unencrypted messaging platforms.
- Data breaches involving safeguarding data must be reported to your national data protection authority within 72 hours if they are likely to result in a risk to the rights and freedoms of the individuals involved. Notify the DSL and board immediately if a breach is suspected.

6. Pseudonymisation in Practice

Pseudonymisation means replacing real names with reference codes so that case records cannot be linked to identifiable individuals without access to the Identity Index (I1 Part C).

How it works in practice: when a concern is received, the DSL assigns a case reference code (e.g. "Case 2025-07") and individual codes for each party (e.g. "P-001" for the person at risk, "A-001" for the alleged perpetrator). All records — the incident form, the case log, the monitoring plan — use these codes. The only document that links codes to real names is I1 Part C, held only by the DSL and Alternate DSL.

GDPR reference: pseudonymisation is a recognised technical security measure under GDPR Article 4(5) and Article 32. It does not make data anonymous — pseudonymised data remains personal data.



References

GDPR Regulation (EU) 2016/679: Articles 4(5) (pseudonymisation), 5(1)(f) (integrity and confidentiality), 6(1)(b-d) (lawful bases), 9(2)(b-c-g) (special category data), 32 (security), 33 (breach notification).

I1 Incident Form and Log — Parts A, B and C. F0 Section K (Confidentiality). Country Legal Supplement — retention periods by country.

Glossary of Key Terms (Safe Spaces) — for definitions of all bolded terms in this document.



© Safe Spaces, 2026. This material is released under the Creative Commons Attribution 4.0 International licence (CC BY 4.0). Permission is granted to utilize, modify, and translate these resources for organizational use, provided the Safe Spaces project is formally credited. Access the complete toolkit at www.safe-spaces.eu.

Financial support provided by the European Union. Production of this document by the European Commission does not imply endorsement of the material; the perspectives expressed belong solely to the authors. Neither the National Agency nor the Commission accepts liability for any application of the information provided.



Funded by
the European Union

www.safe-spaces.eu