

PERSONAL DATA PROTECTION

“Polish Subsurface Initiative” Foundation

Information notice and personal data processing policy

adopted by decision of the President of the Management Board No. [NUMBER] of

Unofficial English translation. Only the Polish text is legally binding; in case of any discrepancy, the Polish version prevails.

Part I. Information notice

Pursuant to Article 13(1) and (2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), we inform you that:

1. **Controller.** The controller of your personal data is the “Polish Subsurface Initiative” Foundation (Fundacja „Polish Subsurface Initiative”) with its registered seat in Jaworze, address: ul. Złota 2/6, 43-384 Jaworze, Poland, KRS: [KRS NUMBER], e-mail: kontakt@fundacjapsi.com.pl (hereinafter the “Foundation”).
2. **Purposes and legal bases of processing.** Data are processed for the purpose of:
 1. concluding and performing a volunteer agreement, contract or other legal relationship with the Foundation (volunteers, participants in training sessions and events, collaborators, contractors), including conducting volunteer recruitment on the basis of the online application form, cover letter and an interview with the candidate, and keeping the register of volunteers’ engagement points and referring volunteers to training in accordance with the Volunteering Rules — Article 6(1)(b) GDPR;
 2. fulfilling the Foundation’s legal obligations arising in particular from the Act on foundations, the Act on public benefit activity and volunteering, the Act on the National Court Register, accounting and tax regulations (including documenting donations) — Article 6(1)(c) GDPR;
 3. pursuing the Foundation’s legitimate interests: day-to-day communication, handling donors and partners, documenting statutory activity, ensuring safety during events and establishing, exercising or defending legal claims — Article 6(1)(f) GDPR;
 4. for data processed on the basis of separate consent (e.g. image for event reports, contact details for information purposes, data provided by a volunteer candidate beyond what is necessary for recruitment, keeping an application for future recruitment rounds) — Article 6(1)(a) GDPR; consent

may be withdrawn at any time without affecting the lawfulness of processing carried out before its withdrawal;

5. where health data are provided voluntarily (e.g. for diving safety during events) — Article 9(2)(a) GDPR (explicit consent) or Article 9(2)(c) GDPR (protection of vital interests).

3. **Recipients.** Data may be disclosed to entities providing the Foundation with accounting, IT (hosting, e-mail), postal, banking, legal and insurance services — under data processing agreements or as separate controllers, including Google (Firebase services, which host the volunteer application form and the Foundation's panel with the register of volunteers' points, and sign-in with a Google account) — and to public authorities entitled under the law (the registry court, the minister supervising the Foundation, the tax office). Data of members of the Foundation's bodies disclosed in the National Court Register are public by law.
4. **Retention period.** Data of volunteer candidates who were not accepted are kept for 3 months from the final decision (after the time limit for an appeal expires or after the appeal is decided by the Foundation Council) and, with the candidate's consent, for 12 months for future recruitment rounds. Other data are kept for the duration of cooperation and, after it ends, until the expiry of the limitation period for claims and for the periods required by law (accounting and tax records — as a rule 5 years from the end of the year they concern). Details are set out in Part II.
5. **Rights of data subjects.** You have the right to: access your data and obtain a copy, rectification, erasure, restriction of processing, data portability (for data processed on the basis of a contract or consent), object to processing based on Article 6(1)(f) GDPR, and withdraw consent. Requests should be sent to the controller's e-mail or postal address.
6. **Complaint.** You have the right to lodge a complaint with the President of the Personal Data Protection Office (Prezes Urzędu Ochrony Danych Osobowych), ul. Stawki 2, 00-193 Warsaw, Poland.
7. **Voluntary provision of data.** Providing data is voluntary but necessary to conclude an agreement or contract, take part in an event or receive a donation confirmation. Providing data processed on the basis of consent is entirely voluntary.
8. **Transfers and profiling.** The Foundation does not transfer data to third countries or international organisations. In connection with the use of Google services (the Foundation's panel, sign-in with a Google account), data may be processed by Google LLC in the United States — on the basis of the European Commission's adequacy decision (EU-US Data Privacy Framework) or standard contractual clauses (Chapter V GDPR). Data are not subject to automated decision-making, including profiling; decisions on admission to volunteering, awarding points and referral to training are made by people (the President of the Management Board and, on appeal, the Foundation Council).

Part II. Personal data processing policy

§ 1. Scope and controller

1. This policy sets out the rules for processing personal data of the Founders, members of the Foundation's bodies, volunteers, participants in training sessions and events, donors, collaborators and contractors of the Foundation.

2. The controller is the Foundation. The controller's tasks are performed by the President of the Management Board (the Foundation's Management Board has one member). The Foundation is not obliged to appoint a data protection officer and does not appoint one [to be reviewed if the scale of processing changes significantly].

§ 2. Categories of data and purposes

1. The Foundation processes the following categories of data:
 1. identification data: first name and surname and, to the extent required by law (KRS, volunteer agreements, contracts, taxes), PESEL number, date and place of birth;
 2. contact data: residential or correspondence address, e-mail address, telephone number;
 3. cooperation data: functions held in the Foundation's bodies, scope and period of volunteering, participation in events, amounts and dates of donations;
 4. recruitment data of volunteer candidates: data from the application form (first name and surname, telephone, e-mail, cover letter), interview note, decision and any appeal;
 5. register of volunteers' engagement points: event, number of points, use of points for training (training, date of confirmation) and the e-mail address of the Google account used to sign in to the panel;
 6. only with separate consent: image (event reports), data on diving qualifications and experience, health data relevant to diving safety.
2. Data are processed only for the purposes described in Part I point 2, in accordance with the principle of data minimisation.

§ 3. Legal bases

The legal bases for processing are set out in Part I point 2. For each processing operation, the Management Board identifies the appropriate legal basis before processing begins and records it in the record of processing activities, if keeping one is required or done voluntarily.

§ 4. Retention periods

Category of records	Retention period
Volunteer agreements and contracts	duration of cooperation + limitation period for claims (as a rule 6 years from the end of the year in which it ended)
Data of volunteer candidates who were not accepted	3 months from the final decision or, with consent, 12 months
Register of engagement points and their use, volunteer account in the panel	period of volunteering + limitation period for claims (as a rule 6 years from the end of the year in which it ended); the panel account is deleted when the agreement ends
Data of event and training participants	until the event and settlements are completed and, in the event of claims, until the limitation period expires
Donation, accounting and tax records	5 years from the end of the financial/tax year they concern

Category of records	Retention period
Deed establishing the Foundation, resolutions and minutes of bodies containing personal data	for the lifetime of the Foundation (constitutional records)
Data processed on the basis of consent	until consent is withdrawn or the purpose ceases

After these periods, data are deleted or anonymised; paper media are destroyed in a manner that prevents them from being read.

§ 5. Security measures

1. Paper records are kept in a locked place accessible only to the President of the Management Board and persons authorised by them in writing.
2. Electronic records are kept on media or accounts protected by a password and two-factor authentication, with access limited to authorised persons; backups are made. Documents containing personal data stored in the Foundation's repository and on its server are encrypted.
3. Persons allowed to process data act on the basis of a written authorisation and a confidentiality undertaking.
4. Processing is entrusted to external entities (accounting, hosting) only under a data processing agreement compliant with Article 28 GDPR.
5. In the Foundation's panel each person has access only within the scope of their assigned role: a volunteer sees only their own points, their use and the number of points required for training; the register of all volunteers is visible to the President of the Management Board and the Foundation Council, and only the President of the Management Board makes changes.
6. PESEL numbers and addresses of persons cooperating with the Foundation are not published or disclosed to unauthorised persons; attendance lists at events are limited to first name, surname and signature.

§ 6. Exercising rights and data breaches

1. The Management Board handles requests from data subjects without undue delay, no later than within one month (extendable by two months in complex cases, with notice to the requester).
2. If a personal data breach is found, the Management Board assesses the risk, documents the breach in an internal register and, if the breach is likely to result in a risk to the rights or freedoms of natural persons, notifies the President of the Personal Data Protection Office within 72 hours of becoming aware of it; where the risk is high, it also notifies the data subjects.

§ 7. Final provisions

1. The information notice (Part I) is attached to volunteer agreements, volunteer application forms, event registration forms and contracts, and is published on the Foundation's website.
2. The policy is reviewed at least once a year and whenever the scope of processing changes significantly. Amendments to the policy are made by the President of the Management Board.

3. The policy enters into force on the date of its adoption.

"POLISH SUBSURFACE INITIATIVE" FOUNDATION · UNOFFICIAL TRANSLATION – THE POLISH TEXT PREVAILS
GENERATED FROM `rodo.md` · COMMIT 04a4427 · 2026-09-28

