MedSales Academy

https://medsales-academy.sendpulse.courses/

Registered in the Republic of Poland

PERSONAL DATA PROCESSING POLICY

Internal regulatory document · Compliant with GDPR and the law of the Republic of Poland

> *This document has been prepared in accordance with: Regulation (EU) 2016/679 (GDPR); Polish Act of 10.05.2018 on the Protection of Personal Data (Dz.U. 2018 poz. 1000); Act of 18.07.2002 on the Provision of Electronic Services; Act of 16.07.2004 — Telecommunications Law (in the part concerning cookies). Supervisory authority: UODO (Urząd Ochrony Danych Osobowych).*

1. General Provisions and Legal Basis

1.1. This Personal Data Processing Policy (hereinafter — the "Policy") is an internal regulatory document of IHOR HRYTSENKO (hereinafter — the "Controller"), registered in the Republic of Poland, conducting educational activities under the MedSales Academy project.

1.2. The purpose of the Policy is to define the principles, procedures and instruments ensuring the processing of personal data in accordance with the GDPR and related Polish legislation.

1.3. The Policy applies to:

- — all employees and persons acting on behalf of the Controller who have access to personal data;
- — all processors with whom the Controller has concluded a DPA (data processing agreement, Art. 28 GDPR);
- — all personal data processing operations involving customers, prospective customers and partners.

1.4. The Controller appoints a person responsible for data protection (DPO — if Art. 37 GDPR applies) or a person responsible for fulfilling data protection obligations.

2. Record of Processing Activities (RoPA — Art. 30 GDPR)

2.1. The Controller maintains a written record of all personal data processing activities (Record of Processing Activities) in accordance with Art. 30 GDPR, containing:

1. the name and contact details of the Controller and, where applicable, the DPO;

2. the purposes of processing;

3. the categories of data subjects and categories of personal data;

4. the categories of recipients to whom personal data have been or will be disclosed;

5. information on transfers to third countries and the safeguards applied;

6. the envisaged time limits for erasure of data;

7. a general description of technical and organisational security measures (Art. 32 GDPR).

2.2. The RoPA is updated upon any changes to processing operations and provided at the request of UODO.

3. Categories of Personal Data and Data Subjects

Database	Categories of subjects	Categories of data
Clients and users	Natural persons — course purchasers	Name, surname, e-mail, phone, payment data, learning progress, IP
Prospective clients	Persons who submitted an enquiry	Name, e-mail, phone, content of enquiry
Employees	Controller's personnel	In accordance with Polish employment law (separate regulation)
Marketing (with consent)	Newsletter subscribers	E-mail, name, date/method of consent

3.1. The Controller does NOT process special categories of data (Art. 9 GDPR) without the explicit and separate consent of the data subject or in the absence of other grounds provided for in Art. 9(2) GDPR.

3.2. Personal data of children under 16 years of age (in accordance with Art. 8 GDPR and Art. 5 of the Polish Act of 10.05.2018) may only be processed with the consent of parents or legal guardians. MedSales Academy services are intended exclusively for persons who have reached the age of 18.

4. Principles of Personal Data Processing (Art. 5 GDPR)

4.1. All personal data processing operations are carried out in accordance with the following principles:

1. Lawfulness, fairness and transparency (Art. 5(1)(a)) — processing only on lawful grounds and in a manner understandable to the data subject.
2. Purpose limitation (Art. 5(1)(b)) — collection for specified, explicit and legitimate purposes only; further processing incompatible with the original purpose is prohibited.
3. Data minimisation (Art. 5(1)(c)) — only data that are adequate, relevant and necessary are processed.
4. Accuracy (Art. 5(1)(d)) — data are kept up to date; inaccurate data are corrected or erased without delay.
5. Storage limitation (Art. 5(1)(e)) — data are stored in a form enabling identification for no longer than necessary for the purposes of processing.
6. Integrity and confidentiality (Art. 5(1)(f)) — protection against unauthorised processing, loss or destruction.
7. Accountability (Art. 5(2)) — the Controller is able to demonstrate compliance with all principles.

5. Legal Bases for Processing (Art. 6 GDPR) — Detailed Description

5.1. Processing on the basis of consent (Art. 6(1)(a) GDPR):

— Consent is obtained in the form of an explicit affirmative action (opt-in): a checkbox in the registration form, confirmation by e-mail.

— Each purpose — separate consent (marketing is not combined with service terms).

— The Controller documents: who, when, in what manner and for what purpose consent was given.

— Withdrawal is carried out via: account settings, a link in the e-mail, an e-mail request. Withdrawal does not affect the lawfulness of processing prior to withdrawal.

5.2. Processing for the performance of a contract (Art. 6(1)(b) GDPR):

— The basis is a contract with the data subject or measures taken at the data subject's request prior to entering into a contract.

— Provision of data is a necessary condition for receiving the service; without it, performance of the contract is impossible.

5.3. Processing for compliance with a legal obligation (Art. 6(1)(c) GDPR):

— Maintenance of financial records (Polish Act of 29.09.1994 on Accounting).

— Compliance with tax legislation requirements (VAT Act, Income Tax Act).

— Provision of data to authorised authorities on lawful grounds.

5.4. Processing on the basis of legitimate interest (Art. 6(1)(f) GDPR):

— Protection of the Controller against fraud and violations of the terms of use.

— Analytics and improvement of service quality (anonymised statistics).

— Protection of rights in judicial and out-of-court disputes.

— The Controller conducts a documented balancing test for each purpose based on this ground.

6. Consent Management and Withdrawal

6.1. Requirements for valid consent (Art. 7 GDPR):

— Freely given — cannot be made conditional on the provision of a service (except where processing is necessary for its performance).

— Specific — for each purpose separately.

— Informed — clear description of the purpose, categories of data, right to withdraw.

— Unambiguous — expressed through an affirmative action (not pre-ticked boxes, not silence).

6.2. The Controller maintains a register of consents given/withdrawn, indicating: subject ID, date and method of provision, exact text displayed at the time of consent, and date of withdrawal (where applicable).

6.3. Consent to marketing communications is confirmed via a double opt-in mechanism (e-mail subscription confirmation).

6.4. A data subject may withdraw any consent at any time without negative consequences for access to services that do not depend on such consent.

7. Personal Data Retention Periods

Category of data	Retention period	Legal basis
Contractual client data	5 years from contract expiry	Art. 6(1)(b)(c) GDPR + Polish Accounting Act
Payment and fiscal documents	5 years from end of financial year	Polish tax legislation
Marketing consents	Until withdrawal + 3 years for evidence	Art. 6(1)(a) GDPR
Technical logs / security	12 months	Art. 6(1)(f) GDPR
Support requests	2 years after closure	Art. 6(1)(f) GDPR
Inactive accounts	3 years from last activity	Art. 6(1)(f) GDPR
Analytical cookies	13 months	UODO / CNIL recommendations
Security breach data	5 years (documentation)	Art. 33(5) GDPR

7.1. Upon expiry of the retention period, personal data are securely destroyed or anonymised. The destruction procedure is documented.

8. Data Protection Impact Assessment (DPIA — Art. 35 GDPR)

8.1. The Controller conducts a DPIA before commencing processing operations that are likely to result in a high risk to the rights and freedoms of natural persons, in particular:

— systematic and large-scale profiling;

— processing of special categories of data on a large scale;

— systematic monitoring of publicly accessible areas on a large scale.

8.2. If a DPIA indicates a residual high risk, the Controller consults UODO prior to processing (Art. 36 GDPR).

9. Processors and Third Parties (Art. 28–29 GDPR)

9.1. Before engaging a processor, the Controller carries out verification of:

— the existence of technical and organisational measures that comply with the GDPR;

— adherence to the principles of data protection and accountability;

— jurisdiction and relevant mechanisms for transfers to third countries.

9.2. A DPA (data processing agreement) containing the mandatory elements of Art. 28(3) GDPR is concluded with each processor: subject matter, duration, nature and purpose of processing, type of data, categories of data subjects, rights and obligations of the parties.

9.3. A processor may engage sub-processors only with the prior written authorisation of the Controller. The Controller maintains an up-to-date list of processors and sub-processors.

9.4. Sub-processors are required to meet the same data protection requirements as the main processor.

10. Technical and Organisational Security Measures (Art. 32 GDPR)

10.1. Technical measures (taking into account the "state of the art" in accordance with Art. 32(1)):

— Encryption in transit (TLS 1.2+) and at rest (AES-256 or equivalent).

— Pseudonymisation of personal data (where technically applicable).

— Backup with recovery verification.

— Logging of access to personal data.

— Vulnerability management and regular software updates.

— Multi-factor authentication for administrative systems.

10.2. Organisational measures:

— Appointment of responsible persons for different categories of processing.

— Regular staff training (at least once a year) on GDPR and cybersecurity.

— Clear internal procedures for handling data subject requests.

— Security breach response procedure with checklist and timelines.

— Third-party due diligence prior to concluding a DPA.

— Regular internal GDPR compliance audits (at least once a year).

11. Security Breach Response Procedure (Art. 33–34 GDPR)

11.1. Upon detection or suspicion of a personal data breach, the responsible person is obliged to:

1. Immediately record the fact of detection with exact time.

2. Conduct an initial risk assessment for the rights and freedoms of data subjects within 1 (one) hour.

3. If the risk is not negligible — notify UODO within 72 (seventy-two) hours of detection (Art. 33(1) GDPR). If notification is delayed — indicate the reasons.

4. If the risk is "high" — notify the affected data subjects directly without undue delay (Art. 34 GDPR).

5. Document the incident in the breach register with: description of the breach, categories and number of affected data subjects, possible consequences, measures taken.

6. Conduct a post-incident review and implement preventive measures.

11.2. Notification to UODO (Art. 33(3) GDPR) contains: the nature of the breach, categories and approximate number of affected persons, contact details of the DPO, likely consequences, measures taken or planned.

12. Rights of Data Subjects and Internal Procedure for Their Exercise

12.1. A request from a data subject may be received in any form (e-mail, post, verbally). The responsible person registers the request immediately upon receipt.

12.2. Response timelines: 1 (one) month from the date of receipt of the request. For complex requests — extension by 2 (two) months with notification within the first month.

12.3. Verification of the data subject's identity is carried out by means proportionate to the risk of erroneous identification (without allowing excessive collection of additional data).

12.4. If a request is manifestly unfounded or excessive (e.g. repetitive), the Controller may refuse to fulfil it or charge a reasonable fee, documenting the decision.

12.5. The register of data subject requests is retained to demonstrate accountability (Art. 5(2) GDPR).

13. Training and Awareness

13.1. All persons with access to personal data undergo mandatory introductory GDPR training before commencing processing and annual refresher training.

13.2. The training programme covers: GDPR principles, legal bases, rights of data subjects, breach response procedure, secure processing practices.

13.3. Completion of training is documented.

14. Policy Changes and Review

14.1. This Policy is reviewed at least once a year, and also upon: material changes in legislation or UODO recommendations; introduction of new processing operations; identified breaches or audit results.

14.2. All versions of the Policy are archived for at least 5 (five) years.

15. Contact Information

Controller: IHOR HRYTSENKO

Address: Region Śląskie, Gliwice, ul. Czwartaków 11/27, Poland

NIP: 6312731797 / REGON: Śląskie

E-mail: medsales.academyonline@gmail.com

This Policy is approved by the Controller and enters into force on the date of signing.