

WEBSITE DOCUMENTS

Privacy Policy

We explain what information is involved in using our website, why it may be processed and how to exercise your rights.

Draft for approval before publication

1. Controller and contact

The controller of personal data covered by this Policy is VigilHorizon sp. z o.o., ul. 28 Czerwca 1956 r. 400, 61-441 Poznań, Poland; KRS 0001207251, NIP 7831942317, REGON 543322810. For privacy enquiries and rights requests, email privacy@vigilhorizon.pl, call the company's general number +48 61 648 88 00 or write to the company's address.

This Policy covers the website and correspondence concerning its services. It does not replace notices provided to employees, applicants or clients in separate processes. Processing within SOC/NOC services, audits and projects, including data from clients' systems, requires separately defined roles, scope and legal basis and, where necessary, a data processing agreement.

2. Forms and delivery of correspondence

The contact form and needs questionnaire include submission functionality addressed to vigilhorizon@vigilhorizon.pl through dhosting.pl email services (smtp.dpoczta.pl). Messages are sent using the technical account website@vigilhorizon.pl, with your supplied email address used for replies. Until mail server configuration is completed and enabled, the form reports that sending is unavailable and does not submit the enquiry. You can instead contact us directly at the general email address vigilhorizon@vigilhorizon.pl or by telephone.

Once submission is enabled, the server validates the enquiry and anti-spam protection, then hands the message to the mail server. Message content is not stored in a separate forms database in this application; it is processed during submission and by the email service handling correspondence. SMTP acceptance does not mean that a person has read the message, that services have started or that delivery to an inbox is guaranteed.

3. Data categories and sources

We primarily receive contact information directly from the person contacting us. For organisational matters, we may receive a representative's details from that organisation or another participant in correspondence. If data comes from another source, we provide the required source and processing information within the period set by Article 14 GDPR, subject to its applicable exceptions.

- Contact form: organisation name, email address, telephone number and acknowledgement of the personal data notice are required. We also process the selected service area, message content and

information provided during the conversation. Correspondence may include a name and professional role if supplied.

- Needs questionnaire: organisation name, email address and acknowledgement of the personal data notice are required; the telephone number remains optional. It additionally includes optional numbers of servers and computers and interest in SOC selection assistance or an audit. Required fields are marked in each form.
- Technical data: a page request makes information such as the IP address, requested resource and browser headers available to the server handling it. The local server does not keep a visitor access log. The scope and retention of logs on production hosting must be confirmed before publication.
- Do not send passwords, access keys, complete production logs or special-category data such as health information through general contact channels. For sensitive materials, we agree an appropriate channel and access scope.
- Form protection: the anti-spam computation result, short-lived verification identifiers, a pseudonymous IP-address hash for request limiting and submission hashes to prevent duplicates. This data is not used for advertising or user profiling.

4. Purposes and legal bases

GDPR means Regulation (EU) 2016/679. We identify the legal basis according to the specific purpose and our relationship with the individual; we do not rely on a single blanket consent for all correspondence.

- Taking steps at your request before a contract, or performing a contract to which you are a party as an individual: Article 6(1)(b) GDPR, for data necessary for those steps. Representing a company does not itself make you a party to its contract.
- Responding to a general enquiry, corresponding with an organisation's representative and maintaining contact about the matter raised: Article 6(1)(f) GDPR. Our legitimate interest is handling correspondence and business communication, taking account of the individual's rights and reasonable expectations.
- Complying with legal obligations, including handling GDPR rights requests and retaining records required by law where such records arise: Article 6(1)(c) GDPR in conjunction with the relevant obligation.
- Protecting the website and correspondence against misuse and establishing, exercising or defending legal claims: Article 6(1)(f) GDPR. Our interest is security and protection of rights; the data scope must be proportionate to the actual need.
- Separate voluntary activities requiring consent may be based on Article 6(1)(a) GDPR. The current website does not offer newsletter subscriptions. Sending an enquiry, acknowledging this Policy or accepting the Terms does not constitute consent to future marketing. Marketing through channels covered by Article 398 of Poland's Electronic Communications Law requires compliance with that provision.

5. Providing data voluntarily

You do not need to provide contact details to browse the content. Providing information in correspondence is voluntary, but a missing reply address or information needed to understand the matter may prevent us from responding, preparing a proposal or fulfilling a request. You do not need to provide information unrelated to the matter. Obligations arising from a particular law or contract are explained in the relevant process.

6. Recipients and transfers outside the EEA

Handling actual correspondence may require authorised personnel and contractors and hosting, email and IT support providers. Appropriate processing agreements and instructions are required where they act on our behalf. Data may also be disclosed to legal advisers or other authorised recipients where necessary, and to public authorities within the law. We do not sell contact information.

The configured email service uses dhosting.pl; data from an enabled form reaches our mailbox through that provider. ALTCHA runs on the website's infrastructure without disclosing submissions to the ALTCHA operator. The prepared Google Tag Manager integration manages measurement tags and may connect to Google only after analytics consent. The Google Analytics 4 tags configured in the container and receipt of data by that service require separate confirmation. The website hosting provider, the relevant Google entity, processing agreements, processing locations and any access from outside the European Economic Area (EEA) must be confirmed before publication. Without that verification, we do not assert that every process remains exclusively within the EEA.

Before enabling a process involving a transfer outside the EEA, the appropriate basis under Chapter V GDPR must be established, such as an adequacy decision or appropriate safeguards, and information about the mechanism and how to obtain a copy must be provided. Standard contractual clauses alone do not replace an assessment of the transfer conditions and any necessary supplementary measures.

7. How long data is kept

The period depends on the purpose, type of matter and legal obligations. A single period does not apply to all messages and records. Once the purpose ends and no further basis exists, data must be deleted or effectively anonymised; keeping it "just in case" is not a separate purpose.

- Enquiries: for the time needed to respond and close the matter, and longer only as necessary to document arrangements or protect specific legal claims, taking account of the applicable limitation period.
- Business relationships: for the time needed to perform the agreement, followed by retention required by relevant legal obligations or justified protection of claims. Accounting records are subject to applicable statutory periods; this does not impose the same period on all correspondence.
- Consent-based processing: until consent is withdrawn or the purpose ends earlier, subject to retaining information needed to demonstrate compliance. Objections to legitimate-interest processing are considered under Article 21 GDPR.

- Language cookie: session-only, with no persistent retention period set; it can be deleted earlier. Browsers with session restoration may retain the cookie after restarting. The operational retention schedule for email, logs and backups must be confirmed before production deployment.
- Anti-spam mechanisms: an ALTCHA challenge is valid for 5 minutes. Associated verification data and request limits held in memory are automatically cleared within 30 minutes while the server is running. The register of submission hashes and statuses used to prevent duplicate sending has a 24-hour validity period; expired entries are removed on startup and during cleanup cycles of up to 15 minutes. The register contains neither message content nor a plain IP address.

8. Your rights

The scope of your rights depends on the legal basis and circumstances of processing. Send requests to privacy@vigilhorizon.pl or the company's postal address. No special form is required. If we have reasonable doubts about identity, we may request additional information necessary to confirm it; we do not automatically require a copy of an identity document.

- Access to your data and a copy of it, and rectification of inaccurate data or completion of incomplete data.
- Erasure and restriction of processing in the circumstances specified by the GDPR. Erasure is not always possible, for example where retention is required by law or necessary to defend legal claims.
- Portability of data you have provided where processing is based on consent or a contract and carried out by automated means, within the limits of Article 20 GDPR.
- Objecting to legitimate-interest processing on grounds relating to your particular situation. We then stop processing unless we demonstrate compelling legitimate grounds or a need to establish, exercise or defend legal claims. An objection to direct marketing requires no explanation.
- Withdrawing consent at any time where it is the basis for an activity. This does not affect the lawfulness of processing before withdrawal.

9. Response times and complaints

We provide information about action taken on a request without undue delay, generally within one month of receipt. Where necessary because of the complexity or number of requests, the period may be extended by two further months; we explain the extension and its reasons within the first month. If we refuse a request, we explain the reasons and available remedies.

Exercising your rights is generally free of charge. A fee or refusal is permitted only within the GDPR's limits, including for manifestly unfounded or excessive requests where those circumstances can be demonstrated.

You may lodge a complaint with the President of Poland's Personal Data Protection Office (UODO), particularly if you believe processing infringes the GDPR. Current complaint submission methods are available at uodo.gov.pl. Contacting us first may help resolve the matter but is not a condition for lodging a complaint. You also retain the right to a judicial remedy.

10. Cookies, browser storage and preferences

We use a first-party cookie to remember your language selection: `vh_language`, with the value `pl` or `en`. It is set after you manually use the language switch; an existing selection is converted to a session cookie when the page opens. The cookie stores only your language preference for the session and applies within the website; it uses `SameSite=Lax` and, over `HTTPS`, `Secure`. It contains no name, email address or advertising identifier.

It restores the language you expressly selected. This specific mechanism is treated as necessary to provide the requested function under Article 399(3)(2) of Poland's Electronic Communications Law; that exception does not extend to analytics or advertising. Without a saved preference, the website reads the browser language: Polish leads to `/pl/`, other languages to `/en/`, and no language information to the Polish default. A direct `/pl/` or `/en/` address lets you choose a version.

We store your analytics choice in the browser's `localStorage` under `vh_analytics_consent`. The record contains your acceptance or refusal, the time of your choice and the consent policy version. It is read for up to 180 days or until that version changes. It restores your decision and contains neither form contents nor an advertising identifier. The setting applies to the particular browser and website origin. You can change it through Privacy settings in the footer or delete it in the browser; after deletion, a new choice is needed before analytics can start again. This period does not determine the lifetime of any GA4 cookies or data retention in Google.

You can delete or block the cookie in your browser settings. The website remains available, but may not remember your selection on a later visit. The service catalogue search places the query and filter in the page address, so they may appear in browser history or a shared link. Do not enter confidential information in the search.

11. Analytics, anti-spam protection and links

Google Tag Manager (GTM) manages measurement tags. We have prepared its integration with the analytics consent mechanism. GA4 is the planned recipient of website usage data; availability of the public container script and connecting GTM alone do not confirm the configuration of GA4 tags or receipt of events by Google Analytics. Sending data requires appropriate configuration and verification. A container can contain additional tags, so their actual scope and consistency with this Policy must be checked before deploying this version of the website.

On the target domain, GTM scripts and Google tags are blocked until you voluntarily consent to analytics. Before a choice and after refusal given before those tools load, we send neither analytics data nor a container download request to Google. Equally prominent buttons allow you to accept or refuse; refusal does not restrict content or contact options. Privacy settings in the footer let you change your decision. Withdrawal stores a refusal, stops the website from forwarding new events and removes recognised GA cookies accessible to the page. If the container has already loaded, the document reloads to restore the block on its execution. This does not erase data already transmitted. Consent-based processing takes account of Article 6(1)(a) GDPR and Article 399 of Poland's Electronic Communications Law.

Downloading the GTM container after consent connects to Google infrastructure and transmits technical request information. This is not evidence that GA4 has received events. Before publication and

measurement activation, we will complete information about the relevant Google entity, recipients, the basis for transfers outside the EEA, actual cookies and their lifetimes, and data retention. Cookie lifetime is different from user and event data retention in GA4; those settings do not apply in the same way to aggregated reports. Events prepared by the website contain no message contents, email addresses, phone numbers, search terms, URL query parameters or fragments. GTM tags and GA4 automatic measurement must also be checked to prevent them from extending that scope.

We selected ALTCHA hosted on the website's infrastructure to protect enabled forms, without an account with an external CAPTCHA provider. The browser performs a computation and our server verifies the result. In this configuration, ALTCHA does not set cookies, collect pointer or scrolling behaviour signatures or send data to the ALTCHA operator. Verification and submission limits protect against abuse under Article 6(1)(f) GDPR. If verification does not work on your device, you can contact us by email or telephone.

Links to Clutch, Facebook, X, LinkedIn and other sites are ordinary links. Once you activate a link, the external operator handles your visit under its own policy. Article sharing buttons pass the selected article address and, for X, its title. The external operator may receive technical connection information.

The scope described in this Policy covers statistical analytics rather than advertising profiling. It does not provide for decisions based solely on automated processing that produce legal or similarly significant effects for users. Additional purposes or tags require prior assessment of the legal basis, appropriate information and any required consent.

12. Security and updates

Safeguards must match the risk, nature of the data and actual configuration, including access controls and secure correspondence handling. The local HTTP preview does not represent the security of production hosting. HTTPS configuration, permissions, backups, incident handling and provider agreements must be confirmed before publication. No website statement guarantees the complete elimination of risk.

Document version: 18 October 2026. We update this Policy when the law, website features or data processing change. Material changes to purposes or practices are communicated as appropriate; a new version alone does not replace required consent or another legal basis. The current version is available on the website and as a PDF.

Legal basis and sources

Links lead to official publications. Read this document together with its version and status information.

[GDPR - Regulation \(EU\) 2016/679](#)

[Polish Electronic Communications Law - Articles 398-400](#)

[UODO - data subject rights](#)

[UODO - how to lodge a complaint](#)

[Article 29 Working Party - cookie consent exemptions, Opinion 04/2012, section 3.6](#)

[Google - consent mode behaviour](#)

[Google Analytics - data retention](#)

[Google - data processing terms](#)

[ALTCHA - self-hosted widget configuration](#)

[dhosting.pl - SMTP and STARTTLS configuration](#)