# Privacy Policy – baycode.eu

**Effective Date:** January 3th, 2024

Thank you for choosing to engage with baycode.eu. This Privacy Policy outlines how I handle your data to ensure your privacy and security.

**Data Collection Officer:**
**Krystian Bajno** - info@baycode.eu.

*Note: In this Privacy Policy, the Data Collection Officer, Krystian Bajno, will be referred to as "Baycode."*

**Your responsibilities:**
- Read this Privacy Policy
- If you provide us with personal information about other people, or if others give us your information, we will only use that information for a specific reason for which it was provided to us. By submitting the information, you confirm that you have the right to authorize us to process it on your behalf in accordance with Privacy Policy
- You have the right to withdraw consent at any time.
- You have the right to lodge a complaint with a supervisory GDPR authority.
- You have the right to request Baycode for copies of your personal data in encrypted form and decrypted form.
- You have the right to request to correct any information you believe is inaccurate.
- You have the right to erase your personal data.
- You have the right to restrict Baycote to process your personal data.
- You have the right to object to processing of your personal data.
- You have the right to request that Baycode transfer the data that we have collected to another organization, or directly to you, under certain conditions.

**Our responsibilities:**
**Data Collection**
Your data is being collected only in the contact form. What you type in, we will process. Data such as Full Name, email, phone numbers, and messages are being collected, but you are free to put in anything you want, as the form fields are loosely validated.

If you agree, we will share your data in encrypted form with Amazon – on a specific AWS S3 bucket, and nobody else than Baycode will be able to read it.

**How will we use your data:**
We will process your message and respond to your communication on a specified channel by you.

**Retention period**
Retention period for data is 2 years. After that, all the messages are going to be deleted using automatic script regardless of encryption or not.

**Cookies**
Cookies are text files placed on your computer to collect standard Internet log information and visitor behavior information. **We are not making use of any cookies on the website.**

**Automatic decision making system**
Another factor being used is the Google reCAPTCHA, that informs the contact form, that you are not an automated software trying to flood the form. The CAPTCHA data is not being persisted anywhere by Baycode.

**Privacy policies of other websites**
The **Baycode** website contains links to other websites. Our privacy policy applies only to our website, so if you click on a link to another website, you should read their privacy policy.

**Marketing**
**Baycode** would send you information about products and services only directly after submitting the form and establishing communication, without further adding you to any marketing lists. You have the right at any time to stop me from contacting you for marketing purposes.

**Provision of data contract**
The provision of data is unnecessary without using the contact form. The encrypted data is passed to Amazon S3 private bucket.

**Data Processing**
Your messages submitted through our contact form are processed with the utmost care and security measures:
• **Encryption**: Your message is AES-256 CBC encrypted using a randomly generated symmetric key during transmission.
• **Transmission**: The encrypted message is sent securely through Vercel serverless cloud function.
• **Storage**: The cloud function stores the encrypted message along with RSA encrypted symmetric key.
• **Notification**: We receive your message as soon as you click the submit button.
• **Decryption**: Upon receipt, we decrypt the key using our offline private key and then decrypt the message using the symmetric key using a custom client.
• Envelope Encryption: This technique ensures secure transmission and storage of your data.

Exposing the encryption algorithm does not compromise security, provided the private key remains confidential.

**Data Storage**
Your encrypted contact information is treated with care:
• **Storage Location:** Your encrypted contact info is stored exclusively in a private S3 bucket.
• **Third-Party Sharing:** We do not send your data elsewhere without your explicit permission

**Key Loss Impact**
In the event of a private key loss:
• **Unreadable Messages:** Previous messages become unreadable, similar to an inaccessible crypto wallet.
• **Recovery:** We regenerate a new RSA pair and redeploy the cloud function promptly to restore the form's operational status.
• **Key Rotation:** Regular key pair rotation is implemented as a good practice.

**Security Measures**
We prioritize the security of your data:
• **Breach Protection:** A breach of our cloud account or Telegram (Telegram FZ LLC) account will not expose your data.
• **Limited Exposure:** Attackers would only obtain public keys or mangled data; the private key is stored safely offline.
• **No Confidential Data**: No confidential information is stored on our website, nor is it accessible from the cloud provider.
• **Leak handling**: In occurrence of encrypted data leak, the GDPR authorities will be notified.

**Website Functionality**
Our website operates with your security in mind:
• **Reboot Mechanism**: The serverless website, like the cloud function, reboots from Vercel storage when accessed.
• **No Permanent Hosting**: We do not engage the website https://baycode.eu in permanent hosting or visitor logging.

**Contact Us**
If you have any questions or concerns regarding our privacy practices, please contact us at info@baycode.eu

**Changes to this Privacy Policy**
We reserve the right to update this privacy policy.
Please check back periodically for any changes.

The most recent revision will be reflected in the effective date.

Thank you for reaching out to us!
Baycode, https://baycode.eu

**How to contact the appropriate authority**
Should you wish to report a complaint or if you feel that we had not addressed your concern in a satisfactory manner, you may contact the Information Commissioner's Office at
https://uodo.gov.pl/en/p/contact

**Personal Data Protection Office**
ul. Stawki 2, 00-193 Warszawa
+48 22 531 03-00
Working hours of the office: 8 a.m. – 4 p.m.

The Office's chancellery operates from 8.00-15.00
kancelaria@uodo.gov.pl

**Infoline (in Polish):**
+48 606 950 000 Operates on weekdays from 10.00 – 14.00