

## PRIVACY POLICY

Regarding the processing of personal data within the whistleblowing channel IntegrityLog

### **New Sources Energy N.V.**

Adopted by the Board on 14 October 2024

## PRIVACY POLICY

New Sources Energy N.V.'s (the **Company**) goal is to comply with its corporate governance obligations and to conduct all business activities in a transparent and prudent way, and with integrity towards all of its stakeholders. These values are also found in the Company's other policies.

The purpose of the whistleblowing channel is to provide employees with the possibility to report severe misconducts which have occurred or are likely to occur in our organisation, without a risk of being subject for retaliation. It is an important tool for reducing risks and maintaining trust in our operations by enabling us to detect and take action at an early stage. The whistleblowing channel (the "**Channel**") is provided by Euronext Corporate Services Sweden AB (the "**Service Provider**"), an external and independent actor. The Channel allows employees to file anonymous reports.

This privacy policy describes how we collect and use your personal data (as defined in the General Data Protection Regulation (EU) 2016/679, the "**GDPR**") to fulfil our legal obligations according to Directive (EU) 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union law (the "**Directive**") and relevant implementing national laws (e.g., the Swedish Act on Whistleblowing (2021:890)), and applicable rules on data protection. This privacy policy also describes your rights and how to enforce them.

Further information about the whistleblowing team and the handling of whistleblower matters can be found in the whistleblowing guidelines.

If you have any questions or comments on your privacy and our processing of your personal data as described herein, you can reach us by emailing us.

In addition to our processing of your personal data as a data controller described herein, our Service Provider may, in conjunction therewith, process additional personal data (such as account login credentials) for which the Service Provider is the data controller. For more information hereof, please read the Service Provider's privacy policy here.

### 1. PERSONAL DATA THAT WE PROCESS, PURPOSE FOR THE PROCESSING, AND THE LEGAL BASIS

<b>Personal data that we may process</b>	<ul style="list-style-type: none"> <li>• Name, telephone number, address, e-mail address of the whistleblower;</li> <li>• Information about the subject of the whistleblowing report, e.g., name and contact details of the person who is the subject of the report, a description of the violation or abuse, time and place and all other information that the notifier considers relevant (depending on the nature of the notification, the personal data processed may contain personal data belonging to special categories of personal data);</li> <li>• Names and contact details of any witnesses or other people involved in the case;</li> </ul>
--	---

	<ul style="list-style-type: none"> <li>• Information on how notifications are made, processed, and communicated (including notification code and status);</li> <li>• Other information provided by the notifier that contains personal data;</li> <li>• Information about those who process notifications that come through the Channel, e.g., name, job title, email address, user ID.</li> </ul>
<b>Purpose for the processing</b>	<ul style="list-style-type: none"> <li>• To implement the Channel and to process the reports received, to monitor and investigate irregularities and, if necessary, to prepare, bring, or defend a legal claim.</li> </ul>
<b>Legal bases for the processing</b>	<ul style="list-style-type: none"> <li>• To fulfill our legal obligation (Article 6(1)(e) of the GDPR);</li> <li>• Our legitimate interest in ensuring the legality and ethics of our operations (Article 6(1)(f) of the GDPR);</li> <li>• In cases where such notifications contain information about special categories of personal data, the processing of such information is necessary to prepare, file or defend a legal claim in accordance with Article 9(2)(f) of the GDPR.</li> </ul>

## 2. HOW WE COLLECT YOUR PERSONAL DATA

The information comes from the person who files a report and can be supplemented with information needed for the investigation. In such case, the information comes from us or a third-party source to verify the information received.

## 3. HOW WE SHARE YOUR PERSONAL DATA

Your personal data may be shared to:

- **Lawyers and legal process.** In addition to our whistleblowing team, lawyers or other experts and internal auditors approved by the company may be involved in the processing and follow-up of whistleblowing reports. In addition, information may be disclosed in accordance with the law, for example to the police in connection with a criminal investigation. Without the express consent of the notifier, the identity of the notifier shall not be disclosed to persons other than those responsible for receiving and following up on reports. However, the identity of the notifier may be disclosed if it is necessary for the competent authority to be able to determine the validity of the notification, for the investigating authorities or the prosecutor to be able to carry out their tasks or to prepare, present or defend a legal claim. We will inform the reporter in advance that his/her identity is to be disclosed, unless such information would jeopardize the investigation of the accuracy of the report or the related preliminary investigation or trial.

- **Our Service Provider.** Your personal data will be shared with our Service Provider in order to provide the Channel. Our Service Provider is not authorised by us to use or disclose your personal data except as necessary to provide the Service or to comply with legal requirements. We do not permit any suppliers or subcontractors to use your personal data that we share with them for marketing purposes or for any other purpose than in connection with the services they provide to us.
- **Merger, acquisition, or other business transfer.** We may share or transfer your personal data in connection with any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.

#### 4. WHERE WE PROCESS YOUR PERSONAL DATA

We always strive to process and store your data within the EU/EEA. However, your data may in certain situations be transferred to relevant recipients as described above, on a need-to-know basis. For example, we may be legally obligated to share your personal data with authorities both in the country where you and we are domiciled and abroad. This could mean that your personal data is transferred to third countries outside the EU/EEA territory.

Please note that privacy laws in countries outside of the EU/EEA may not be the same as, and in some cases may be less protective than, privacy laws in your country. However, we always select our service providers carefully and take all the necessary steps to ensure that your personal data is processed with adequate safeguards in place in accordance with the GDPR.

#### 5. HOW LONG WE KEEP YOUR PERSONAL DATA

The data is saved for the maximum of the legal retention time in national law after the end of the whistleblower case (e.g., 2 years in Sweden). After that period, your personal data will be erased or anonymised, unless we are legally obliged to keep it.

The log of submitted reports containing the names of people involved in the investigations will be stored for compliance audit purposes for 10 years, after which the need for additional storage will be assessed.

#### 6. YOUR RIGHTS

- **Right to information and access to your data.** You have the right to request information about how we process your data and a transcript of personal data processed by us. The first transcript may be requested free of charge, however if you make repeated and unreasonable requests for copies, we might charge you with an administrative fee. As the person reporting, you have the right to receive information once a year, free of charge, about which personal data is registered about you in the Channel. Such request for an extract from the register must be made in writing and signed.
- **Right to rectification.** You have the right to correct inaccurate or incomplete information about yourself.
- **Right to erasure ('right to be forgotten').** You have the right to request that we erase personal data about you, for example if the data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, or if there is no legal basis for processing the data.

- **Right to restriction.** You are entitled to request that the processing of your personal data should be limited until inaccurate or incomplete information about you has been corrected, or until an objection from you have been handled.
- **Right to object.** You have right to object to processing based on legitimate interest. This means that we may no longer process the personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests.
- **Right to withdraw your consent.** You may at any time withdraw any consent you have given us. However, please note that it will not affect any processing that has already taken place.
- **Right to complain.** You have the right to lodge a complaint to the Supervisory Authority in the country you live or work in, if you believe that we have not complied with our obligations regarding your personal data. In Sweden, the Supervisory Authority is the Swedish Authority for Privacy Protection.

Please note that our legal rights or obligations may prevent us from disclosing or transfer all or part of your information, or from immediately deleting your information.

Please contact us using the contact details at the top to exercise any of your rights.

## 7. DEROGATIONS TO THE DATA SUBJECT RIGHTS

Access right does not apply to data that can reveal the identity of the whistleblower.

Note also that according to GDPR art 14.5 b the right to access is limited if the information is likely to render impossible or seriously impair the achievement of the objectives of that processing (to investigate a whistleblower case).

## 8. SECURITY MEASURES

The Channel is encrypted, and password protected to ensure the anonymity of the whistleblower. Notifications received through the Channel are only received and handled by authorised personal. No IP addresses are registered in the Channel, and the system does not use cookies. All data communication and storage of personal data is encrypted to prevent them from being distorted or coming to the knowledge of unauthorised persons.

## 9. CHANGES TO THIS PRIVACY POLICY

We might change and update this privacy policy. In case of any material changes to this privacy policy or our processing of your personal data, we will inform you of such changes.

\*\*\*