

Södra's Personal Data Protection Notice – whistleblowing

1. INTRODUCTION

Södra is a data controller for the processing of your personal data whenever you submit a report, or are party to a report submitted, to our whistleblowing system.

For the purpose of this Personal Data Protection Notice, “**Södra**” refers to the following company: Södra Skogsägarna ekonomisk förening (Corporate Identity Number: 729500-3789).

All references to “we,” “us” and “our” in this Personal Data Protection Notice shall be considered a reference to Södra. You can find our contact details at the end of this Personal Data Protection Notice.

We respect your privacy and are committed to protecting your personal data.

2. SCOPE OF THIS PERSONAL DATA PROTECTION NOTICE

This Personal Data Protection Notice refers to Södra's processing of personal data for individuals who submit a report, and who are party to a report submitted, to our whistleblowing system. This Personal Data Protection Notice contains information such as the purposes for which we process personal data, with whom we share your data, and your rights in relation to your personal data.

3. WHAT CATEGORIES OF PERSONAL DATA DO WE PROCESS, FOR WHAT PURPOSE AND ON WHAT LAWFUL BASIS?

Södra processes personal data in the manner and for the purposes set out in the tables below. The tables below also present the lawful basis on which we base our processing for each purpose, and the length of time that we will retain your personal data.

Purpose:	The personal data that we process:
<p>We will investigate misconduct and suspected irregularities within our organisation in the form of internal policy breaches. For this purpose, we will manage, follow up and document the content of the whistleblowing reports and any subsequent issues. We will collect and review information from the IT devices and digital systems that you</p>	<ul style="list-style-type: none"> • Contact details including name, telephone, address and e-mail address. • Date of birth. • Reporting history and report number. • Employment details (including role and responsibilities). • Images and audio recordings. • Communication history. • Internet history.

<p>use within the scope of your employment, and that we control. We will also interview any individuals who are relevant to the investigation and, if applicable, contact the relevant authorities for the investigation.</p>	<ul style="list-style-type: none"> • User history from the IT devices and digital system that you, as an employee, use within the scope of your employment and that we control. • Personal data related to actions in breach of our Code of Conduct and internal policies.
<p>Lawful basis:</p>	
<p><i>Legitimate interest.</i> Processing is necessary for the purpose of our legitimate interest to ensure compliance with the internal policies of our company.</p>	
<p>How we share and transfer your data:</p>	
<p>For the purposes specified above, Södra will share your personal data with the following recipients:</p> <ul style="list-style-type: none"> • relevant authorities, • our IT provider of the whistleblowing channel (Whistleblower Software ApS); and • Södra’s external legal representatives (such as PwC). <p>to the extent that is necessary for them to provide their services to us.</p> <p>Södra may transfer your personal data to a so-called third country (a country outside the European Union (EU)/ European Economic Area (“EEA”) within the scope of this processing activity, in the event that a whistleblowing report submitted to Södra’s whistleblowing channel is a cross-border case. A whistleblowing report is cross-border if either the person submitting the report, or a person who is party to the report submitted and/or the investigation, such as a witness, is employed by Södra in a country outside the EU/EEA. In this event, Södra may need to share any relevant details, including your personal data, with recipients in the following third countries: The US, the UK and China.</p> <p>For more information, refer to Section 5 about the safeguards we put in place to protect your personal data when transferring it to a third country. You are also welcome to contact us via info@sodra.com if you have concerns related to the transfer of your personal data to a third country.</p>	
<p>Storage period:</p>	
<p>We process your personal data for the time that is necessary until the matter for which the whistleblowing channel has been used is closed or, otherwise, for the time that is necessary for the establishment, exercise or defence of legal claims.</p>	

Purpose:	The personal data that we process:
<p>We will manage reports of breaches of internal policies by collecting and administering reports received via the whistleblowing channel. We will also communicate with the people affected by the reports. We will manage, follow up and document the contents of the report and any subsequent issues. We will do this in order to properly address reports of possible breaches of internal policies.</p>	<ul style="list-style-type: none"> • Contact details including name, telephone, address and e-mail address. • Date of birth. • Reporting history and report number. • Employment details (including role, identification and responsibilities). • Images and audio recordings. • Personal data related to actions in breach of our Code of Conduct and internal policies.
Lawful basis:	
<p><i>Legitimate interest.</i> Processing is necessary for the purpose of our legitimate interest to ensure compliance with the internal policies of our company.</p>	
How we share and transfer your data:	
<p>For the purposes specified above, we will share your personal data with the following recipients:</p> <ul style="list-style-type: none"> • relevant authorities, • our IT provider of the whistleblowing channel (Whistleblower Software ApS); and • Södra's external legal representatives (such as PwC) <p>to the extent that is necessary for them to provide their services to us.</p> <p>Södra may transfer your personal data to a so-called third country (a country outside the EU/EEA) within the scope of this processing activity, in the event that a whistleblowing report submitted to Södra's whistleblowing channel is a cross-border case. A whistleblowing report is cross-border if either the person submitting the report, or a person who is party to the report submitted and/or the investigation, such as a witness, is employed by Södra in a country outside the EU/EEA. In this event, Södra may need to share any relevant details, including your personal data, with recipients in the following third countries: the US, the UK and China.</p>	

For more information, refer to Section 5 about the safeguards we put in place to protect your personal data when transferring it to a third country. You are also welcome to contact us via info@sodra.com if you have any concerns related to the transfer of your personal data to a third country.

Storage period:

We process your personal data for the time that is necessary until the matter for which the whistleblowing channel has been used is closed or, otherwise, for the time that is necessary for the establishment, exercise or defence of legal claims.

Purpose:	The personal data that we process:
<p>We manage reports of breaches of law that are submitted via the whistleblowing channel by collecting and administering the reports. We will also communicate with the people affected by the reports. We will manage, follow up and document the contents of the report and any future issues. We will do this in order to properly address all reports of suspected or actual breaches of law.</p>	<ul style="list-style-type: none"> • Contact details including name, telephone, address and e-mail address. • Date of birth. • Reporting history and report number. • Employment details (including role and responsibilities). • Images and audio recordings. • Personal data concerning criminal convictions, suspected and/or actual breaches of law.
Lawful basis:	
<p><i>Legal obligation:</i> The processing of your personal data is necessary under the Swedish Act on the Protection of Persons Reporting Irregularities (2021:890). Södra is unable to comply with a legal obligation unless the personal data is processed.</p>	
How we share your data:	
<p>For the purposes specified above, Södra will share your personal data with the following recipients:</p> <ul style="list-style-type: none"> • relevant authorities, • our IT provider of the whistleblowing channel (Whistleblower Software ApS); and • Södra’s external legal representatives (such as PwC) 	

to the extent that is necessary for them to provide their services to us.

Södra may transfer your personal data to a so-called third country (a country outside the EU/EEA) within the scope of this processing activity, in the event that a whistleblowing report submitted to Södra’s whistleblowing channel is a cross-border case. A whistleblowing report is cross-border if either the person submitting the report, or a person who is party to the report submitted and/or the investigation, such as a witness, is employed by Södra in a country outside the EU/EEA. In this event, Södra may need to share any relevant details, including your personal data, with recipients in the following third countries: the US, the UK and China.

For more information, refer to Section 5 about the safeguards we put in place to protect your personal data when transferring it to a third country. You are also welcome to contact us via info@sodra.com if you have any concerns related to the transfer of your personal data to a third country.

Storage period:

We process your personal data for the storage period required by law, which is no longer than two years after closing the matter for which the whistleblowing channel has been used or, otherwise, for the time that is necessary for the establishment, exercise or defence of legal claims.

Purpose:	The personal data that we process:
<p>We will conduct investigations into any misconduct and suspected criminal offences that have taken place within our organisation in the form of suspected or actual breaches of law, in order to properly address all suspected breaches of law within our organisation. To achieve this, we will manage, follow up and document the content of whistleblowing reports and any subsequent issues. We will collect and review information from the IT devices and digital systems</p>	<ul style="list-style-type: none"> • Contact details including name, telephone, address and e-mail address. • Date of birth. • Reporting history and report number. • Employment details (including role and responsibilities). • Images and audio recordings. • Communication history. • Internet history. • User history from the IT devices and digital system that you, as an employee, use within the scope of your employment and that Södra controls.

<p>that you use within the scope of your employment, and that Södra controls. We will also interview any individuals who are relevant to the investigation and contact the relevant authorities for the investigation.</p>	<ul style="list-style-type: none"> • Personal data concerning criminal convictions, suspected and/or actual breaches of law.
<p>Lawful basis:</p>	
<p><i>Legal obligation:</i> The processing of your personal data is necessary under the Swedish Act on the Protection of Persons Reporting Irregularities (2021:890). Södra is unable to comply with a legal obligation unless the personal data is processed.</p>	
<p>How we share your data:</p>	
<p>For the purposes specified above, we will share your personal data with the following recipients:</p> <ul style="list-style-type: none"> • relevant authorities, • our IT provider of the whistleblowing channel (Whistleblower Software ApS); and • Södra’s external legal representatives (such as PwC) <p>to the extent that is necessary for them to provide their services to us.</p> <p>Södra may transfer your personal data to a so-called third country (a country outside the EU/EEA) within the scope of this processing activity, in the event that a whistleblowing report submitted to Södra’s whistleblowing channel is a cross-border case. A whistleblowing report is cross-border if either the person submitting the report, or a person who is party to the report submitted and/or the investigation, such as a witness, is employed by Södra in a country outside the EU/EEA. In this event, Södra may need to share any relevant details, including your personal data, with recipients in the following third countries: the US, the UK and China.</p> <p>For more information, refer to Section 5 about the safeguards we put in place to protect your personal data when transferring it to a third country. You are also welcome to contact us via info@sodra.com if you have any concerns related to the transfer of your personal data to a third country.</p>	
<p>Storage period:</p>	
<p>We process your personal data for the storage period required by law, which is no longer than two years after closing the matter for which the whistleblowing channel</p>	

has been used or, otherwise, for the time that is necessary for the establishment, exercise or defence of legal claims.

4. HOW DO WE OBTAIN YOUR PERSONAL DATA?

We process the personal data obtained directly from you when using the whistleblower system or, alternatively, that has been provided within the framework of a report or an investigation.

5. WILL WE TRANSFER YOUR PERSONAL DATA TO A COUNTRY OUTSIDE THE EU/EEA?

We always aim to process your personal data within the EU or the EEA. If we transfer your personal data, in such cases as set out in the tables above, we are responsible for ensuring that your data will be transferred in accordance with applicable data protection legislation before it takes place. These safeguards include ensuring that the country in which the recipient is located can ensure an adequate level of data protection according to the European Commission, or ensuring appropriate data protection safeguards based on the use of standard contractual clauses as adopted by the European Commission and other appropriate safeguards to protect your rights and freedoms.

You can find a list of the countries that the European Commission has decided offer an adequate level of data protection [here](#).

You can find the European Commission's standard contractual clauses [here](#).

6. YOUR RIGHTS

In this section, we set out your rights as a data subject. You can exercise them by using the contact information at the end of this document to contact us. Please note that not all of the rights set out below are absolute, and there may be some exemptions. Your rights are as follows:

- *Right of access*

You have the right to request a copy of the personal data concerning you that we process and to receive additional information about how we process your data.

- *Right to rectification*

You have the right to have inaccurate personal data rectified or incomplete personal data completed.

- *Right to erasure*

You have the right to request that we erase your personal data without undue delay where one of the following grounds applies: (i) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed; (ii) you withdraw your consent on which the processing is based and there is no other

legal ground for the processing; (iii) you object to the processing of your personal data, and we have no overriding legitimate grounds for the processing; (iv) the personal data have been unlawfully processed; or (v) your personal data must be erased for compliance with a legal obligation.

- *Right to restriction of processing*

You have the right to restrict the processing of your personal data where one of the following applies: (i) you contest the accuracy of your personal data for a period enabling us to verify the accuracy of the personal data; (ii) the processing is unlawful and you oppose the erasure of your personal data and request restriction of use instead; (iii) the personal data is no longer needed for the purposes of the processing, but is required for the establishment, exercise or defence of legal claims; or (iv) you have objected to the processing of your personal data pending the verification of whether the legitimate ground for our processing override your interests, rights and freedoms.

- *Right to object*

You have the right to object to our processing of your personal data based on our legitimate grounds. If you object and we believe that we may still process your personal data, we must demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms, or for the establishment, exercise or defence of legal claims.

7. COMPLAINTS TO THE SUPERVISORY AUTHORITY

The data protection authority in Sweden is the **Swedish Authority for Privacy Protection (IMY)**. If you feel that our processing does not comply with the applicable data protection legislation, we urge you to contact us first so that we can review your complaint. You can lodge a complaint with the IMY at any time.

8. CONTACT US

If you have any questions about how we process your personal data or would like to exercise any of your rights, please contact us at:

Södra Skogsägarna ekonomisk förening,

E-mail: info@sodra.com