Document No. 1.13.002

Valid from 30 August 2024

WHISTLEBLOWING PROCEDURE

The public limited company Barrus (hereinafter ‘Barrus’) values honest, transparent, and goal-oriented professional culture. The important pillars of such culture are law-abiding, observant, and motivated employees. Barrus prioritises people who care about each other’s safety and well-being while respecting each other and the law. Achieving the values of Barrus as a company is only possible when each and every employee contributes towards it.

For Barrus as an employer to detect all infringements that take place at work or related to work as early as possible, it has created a tip line for reporting possible breaches and for protecting whistleblowers pursuant to the Protection of Persons Reporting Work-Related Breaches of European Union Law Act (in Estonian *Tööalasest Euroopa Liidu õiguse rikkumisest teavitaja kaitse seadus*; hereinafter, ‘the Whistleblower Act’).

This procedure clarifies the nature of the Barrus tip line and the steps for reporting a breach when it is discovered. All individuals who are not a part of Barrus and who want to report a potential breach are recommended to review this procedure. At the end of the procedure, you will find a diagram for reporting breaches, prepared by the Ministry of Justice, which summarises the contents of this procedure briefly.

1. What type of behaviour should be reported?

The following types of breaches should be reported:

(i) unlawful actions or omissions – such as offering or accepting bribes;
(ii) actions or omissions that are not a violation of the law but contradict the objective of a legal provision.

You must report any of the aforementioned acts if you as an employee of a partner of Barrus (or as a person stipulated in subsection 3 (1) of the Whistleblower Act) have learned about it in relation to your professional activities and you have justified grounds to believe that the breach has just begun or has been completed.

2. When should a breach be reported?

If you notice an action or an omission in a situation that requires action, you must report it immediately. If you are not certain whether the incident you have observed must be reported or not, you may consult a specialist before doing so.

At that, you should keep in mind that the law prohibits knowingly submitting a false report on a violation. Barrus does not tolerate any illegal retaliatory measures against a whistleblower, and similarly, it does not accept any type or form of workplace bullying, including unjustified derogation outside the organisation. If a person knowingly submits a false report on a breach or false information, they can be held liable for a misdemeanour, or in more serious cases, for a criminal offence.

Therefore, if you notice an incident or a situation which should be reported pursuant to this procedure, please do so at the first opportunity, but also keep in mind that submitting a false report knowingly is strictly prohibited.

3. How should an incident be reported?

When reporting an incident, you may choose between an internal and an external channel for reporting.

3.1. Internal channel for reporting

Barrus's internal channel for reporting is an electronic tip line, located at the following link: https://app.guavahr.com/public/feedback/525?token=c5dd735766f9f199c5dd. Any complaints submitted through this tip line are handled by the HR and Working Environment Department and the Management Board of Barrus.

The link may be used for reporting a breach both by identifying yourself or anonymously; in the case of the latter, you must tick the *Send anonymously* box to ensure anonymity.

If you would like to get feedback emailed to you about the breach you have reported, then you must tick the *Subscribe to updates* box. You can receive feedback on your email even if you tick the *Send anonymously* box – in this case, the system will not display your email address to the party handling the report. To receive notifications, you must check whether the entered email address is correct.

If you do not tick the *Subscribe to updates* box, then you will not receive an email notification when a reply has been submitted to your form. However, you are able to see replies to your form through the same link displayed on the website after you have submitted a report, i.e. sent your form. In this instance, make sure you remember to save the link, because without it, you will not be able to see any replies later.

3.2. External channel for reporting

It is also possible to report a breach through an external channel of reporting, independent of Barrus, i.e. to authorities who process or monitor certain types of violations – for example, the Environmental Board handles environmental violations, the Estonian Rescue Board is responsible for fire safety, and the Labour Inspectorate focuses on labour violations. There is no need to submit a report through an internal channel of Barrus prior

to reporting through external channels; in other words, you have the right to choose a suitable channel for reporting.

When selecting a channel for reporting, you should take into consideration which channel would help to eliminate the breach the fastest and the most efficiently, among all else. As a rule, it would be the internal reporting channel; nevertheless, you are free to decide the preferred channel.

In exceptional cases, you have the right to make a public disclosure of the breach; however, it can only be done after:

1) you have already sent a report through an external channel for reporting and the report has not been processed pursuant to the law;

2) the breach is an immediate threat or obvious risk of irreversible damage to public interests;

3) you have grounds to suspect that retaliatory measures are going to be implemented in the case of external reporting;

4) you have grounds to suspect that the breach is not going to be properly processed in the case of external reporting or that the competent authority is involved in the breach.

The confidentiality of the whistleblower is guaranteed regardless of their chosen channel for reporting listed above and only a designated person or a unit has access to the report on the breach and other information related to the incident.

4. Confidentiality and protection

If you report a breach that you have observed in the course of your professional duties, then you can legitimately expect protection. You will be protected if two conditions have been met: 1) at the time of submitting the report, you had reason to believe that the breach

had just begun or had been completed; and 2) you have reported it either through internal channels, external channels, or in justified instances, by informing the public pursuant to this procedure or the Whistleblower Act.

To be granted protection, you must be able to explain while submitting a report which circumstances have led you to believe that a breach has already taken place, is taking place, or has just begun. You do not have to collect evidence about the breach but may do so within reason. Only planning or a hypothetical conversation about committing such an act is not qualified as a prohibited act/omission; however, if you learn of such information, we encourage you to contact the appropriate contact person or the management team of Barrus and share it with them.

The main protection that you will be granted is guaranteeing confidentiality. This means that the party who receives the report (either within Barrus or a representative of an appropriate external channel for reporting) will not disclose any information regarding the whistleblower, thus mitigating the initial risk of illegal retaliation against the person. Disclosure of details regarding the identity of the whistleblower is only permitted with the written consent of the whistleblower.

If you have submitted a report on a breach and the subsequent proceedings determine that the incident did not constitute a breach, you will still be guaranteed protection from retaliation if you believed in earnest at the time of the reporting that the incident entailed a breach. Protection is not guaranteed in the case of submitting a false report knowingly.

5. What happens after submitting a report?

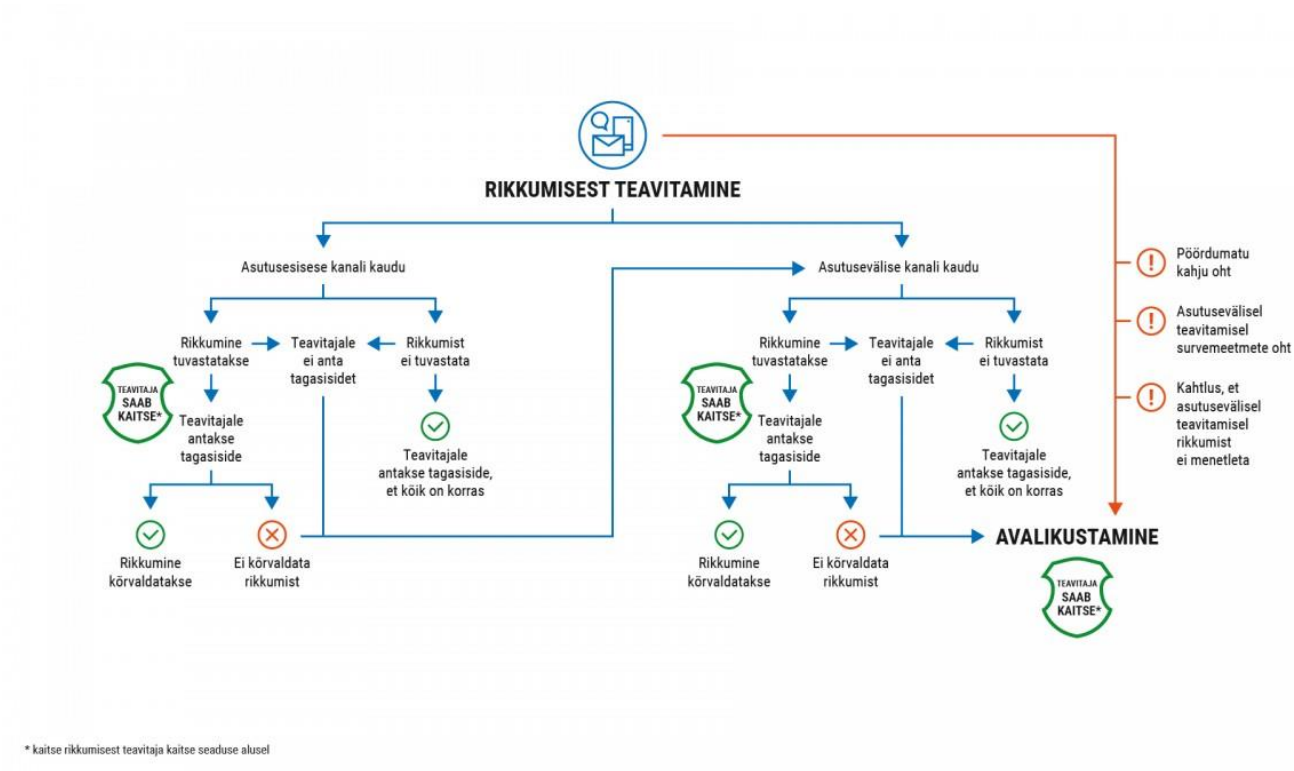
After submitting a report, you will receive a confirmation within seven days, except in instances when you have explicitly prohibited a confirmation being sent to you in the report that you have submitted or when there is reason to believe that it would jeopardise your confidentiality (see the section *How should an incident be reported?* regarding submitting a report).

Feedback on the implementation of follow-up measures will be given internally within three months at the latest, or when reporting through an external channel and in justified instances, within six months after receiving the report on a breach. You will not receive any feedback if you have prohibited it explicitly or there is reason to believe that it would jeopardise your confidentiality.

You will be given feedback about the final result of the proceedings regarding the breach, except in instances when you have explicitly prohibited sending feedback or there is reason to believe that it would jeopardise your confidentiality.

There is no obligation to share feedback if it would violate another legal act.

Moreover, the authority to which you submitted the report may ask for additional details, should the need arise.



AS Barrus; commercial registry code: 10270580
Verijärve, Võru rural municipality
65541 Võru County

Phone: +372 785 0700
Fax: +372 785 0701
Email: info@barrus.ee

RIKKUMISEST TEAVITAMINE	REPORTING A BREACH
Asutusesisese kanali kaudu	Through an internal channel
Rikkumine tuvastatakse	A breach is identified
TEAVITAJA SAAB KAITSE*	**THE WHISTLEBLOWER WILL BE PROTECTED***
Teavitajale antakse tagasiside	The whistleblower will be given feedback
Rikkumine kõrvaldatakse	The breach is eliminated
Rikkumist ei kõrvaldata	The breach is not eliminated
Rikkumist ei tuvastata	No breach is identified
Teavitajale ei anta tagasisidet	No feedback is given to the whistleblower
Teavitajale antakse tagasiside, et kõik on korras	The whistleblower is informed that there is no breach
*kaitse rikkumisest teavitaja kaitse seaduse alusel	* Protection under the Whistleblower Act
Asutusevälise kanali kaudu	Through an external channel
Rikkumine tuvastatakse	A breach is identified
TEAVITAJA SAAB KAITSE*	**THE WHISTLEBLOWER WILL BE PROTECTED***
Teavitajale antakse tagasiside	The whistleblower will be given feedback
Rikkumine kõrvaldatakse	The breach is eliminated
Rikkumist ei kõrvaldata	The breach is not eliminated
Rikkumist ei tuvastata	No breach is identified
Teavitajale ei anta tagasisidet	No feedback is given to the whistleblower
Teavitajale antakse tagasiside, et kõik on korras	The whistleblower is informed that there is no breach
AVALIKUSTAMINE	**PUBLIC DISCLOSURE**
TEAVITAJA SAAB KAITSE*	**THE WHISTLEBLOWER WILL BE PROTECTED**
Pöördumatu kahju oht	Threat of irreversible damage
Asutusevälisel teavitamisel survemeetmete oht	Risk of retaliation when reporting externally
Kahtlus, et asutusevälisel teavitamisel rikkumist ei menetleta	Suspicion that the breach will not be processed in the case of external reporting

AS Barrus; commercial registry code: 10270580
Verijärve, Võru rural municipality
65541 Võru County

Phone: +372 785 0700
Fax: +372 785 0701
Email: info@barrus.ee