WHISTLEBLOWING POLICY

SAS AB (PUBL)

Introduction – what is whistleblowing, and why is it important?

SAS Group strives to achieve transparency and a high level of business ethics. The purpose of the whistleblowing channel is to provide employees with support and guidelines to report severe misconducts which have occurred or very likely to occur in our organization in which an employee is or was in contact through their work, including breaches of our Code of Conduct, 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 act at an early stage.

These guidelines are based on the Swedish Act on Whistleblowing (2021:890) (Sw. Lag om skydd för personer som rapporterar om missförhållanden) (the "Act"), 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 applicable rules on data protection.

The principles set out in these guidelines apply to all of those who are, or have been, in a workrelated context with us, including:

- employees, including trainees/students,
- self-employees/consultants,
- persons subject for recruitment
- shareholders and management who are active in the company, and
- other persons who are/have been in a work-related context with us, under our control and management (hereinafter "employees" or "reporting person").

All employees have a duty to be aware of the contents of these guidelines and any updates to them, and to comply therewith.

All reports made to the whistleblowing channel in accordance with these guidelines will be received, recorded (if orally reported) and processed by the whistleblowing team. The whistleblowing team consists of General Counsel and the Legal Department of Company SAS Group, and oversight by the chairman of the audit committee of SAS AB.

When to blow the whistle?
All employees may report suspected misconducts when a misconduct becomes apparent in our organization.

A "misconduct" means an act or omission occurred (or most likely to occur) in our organization which is considered as harmful to the public interest, which the employee has received knowledge of in a work-related context.

Reporting can also be made where an employee has received knowledge of acts or omissions which are deemed unlawful and constitute a breach according to the Directive, or such breach of regulations as further specified in the Act with reference to Chapter 8 of the Constitution of Sweden (Sw: Regeringsformen).

A breach in the following areas is generally considered as being of "public interest":

- public procurement
- financial services
- products and markets; and the prevention of money laundering and terrorist
- product safety and compliance
- safety or security hazards
- environmental protection
- food and feed safety
- public health
- consumer protection
- harassment or discrimination
- violations of competition laws
- bribes or kickbacks
- breaches of confidentiality
- inappropriate gifts or gratuities

Information of public interest may also be:
- Serious breaches of the SAS Code of Conduct.

If an employee has concerns about their own employment, we ask that the employee discuss the matter directly with their supervisor or HR representative and / or make a report in accordance with our policies. Matters relating to employment and labor law should normally not be reported or dealt with in the procedures of the whistleblowing channel.

How to report
If an employee has reasonable grounds to believe that a misconduct has been made, we encourage all employees to report the matter immediately through our whistleblowing channel.

An employee does not need proof for their suspicion but do however need reasonable cause to assume that the information is true at the time of reporting, and the employee needs to act in good faith. Allegations should not be made with the intent to cause harm.

A report can be provided through the whistleblowing channel which may be found here:

sas.integrity.complylog.com

The channel allows to choose between the following alternatives:

- Oral reporting
- Written reporting
- Reporting by requesting a physical meeting, which shall be enabled within a reasonable time.

It is possible to report anonymously.

Non-relevant information on health status, political or religious beliefs or sexual orientation shall not be included in the report.

Disciplinary actions for intentionally inaccurate reporting
If an employee misuses the reporting procedure by knowingly making inaccurate or malicious allegations, this could be seen as a serious violation, which may result in disciplinary actions.

Prohibition of retaliation
We are committed to a strict policy of non-retaliation, in accordance with applicable law.

The prohibition covers those who, in good faith, report suspected misconducts in accordance with these guidelines, where such misconducts have occurred in a workrelated context or participate in investigations into a matter of misconducts, except where such investigation entails a criminal offence. The prohibition also includes indirect retaliation, such as the employees' colleagues and family members.

Retaliation, termination of employment, dismissal, other unfavorable treatment or other adverse consequences of a person who, in good faith, has reported a misconduct or suspected misconduct in accordance with the provisions of these guidelines shall be considered as a prohibited retaliation.

It is also prohibited to hinder or attempt to hinder a reporting person from reporting information about a misconduct. The same applies if the reporting persons contacts their union in order to discuss prior to reporting.

An employee is also protected when reporting is made internally but not through the established whistleblowing channel, if such whistleblowing channel is missing/ disabled, or is not established in accordance with the Act, or if the employee has not yet commenced their work (under recruitment).

The processing and investigation process

Authority to investigate reports
We are committed to ensure that all reports of suspected misconducts are treated confidential, efficient, and in accordance with our values and applicable law.

The whistleblowing team has exclusive authority and responsibility for internal investigations and performs its duties impartially and independently. People outside the whistleblowing team will be hindered from accessing the reporting channel. However, during the investigation process, the whistleblowing team may also request information and expertise from other individuals within or outside the company (e.g., experts), in which case the obligation to maintain secrecy and confidentiality also applies to them.

The investigation
Reporting through the internal reporting channel is confidential. Information about the identity of the reporting person, the subject of the report and other persons mentioned in the report and other personal data shall be kept confidential.

Information about the identity of the reporting person will not be disclosed to a third party (authority or court), except if necessary, in case of a criminal offence. The information in the report shall be processed as necessary to complete the investigation. Appropriate remedial action, to the extent necessary, shall always be based on the results of a thorough investigation.

In certain circumstances, the whistleblowing team may decide not to investigate the report. This can be the procedure, for example in the following situations:

- the information obtained is insufficient in order to carry out an adequate investigation and no further information is available,
- the report is made in the wrong channel, in which case the reporting person is directed to make the report to the correct party,
- the report is not provided in good faith, or
- if an investigation has already been made.

If the report is made anonymously, the whistleblowing team is prevented from further investigation of the identity of the reporting person. In case of an anonymous report, such report may risk being dismissed if, for example, the information obtained is deemed insufficient in order to initiate an investigation or if the veracity of the information provided cannot be reliably established.

A person who is the subject of a report shall not participate in the investigation or decision-making of the report. If a member of the whistleblowing team is the subject of a report, they may not be involved in the investigation process.

Documentation and data processing
The whistleblowing team is required to document all reports received through the whistleblowing channel and to make sure that the information received is being processed in accordance with the Act and applicable data protection regulations.

Personal data will not be kept longer than necessary, taking into consideration the purpose of handling processing in accordance with the Act.

Personal data shall be deleted after two (2) years following finalized investigation. Finalized investigation will be presented to the management, or such other company representant where there is a risk of conflict.

Further information on the processing of personal data, see Appendix B.

Information to the reporting person and the person subject to the report
Information to the employee shall be provided as follows:

- within seven (7) days following reporting, a confirmation will be sent by the whistleblowing team in order to confirm that the report has been received, except where the employee has expressly requested not to receive any confirmation, or if the whistleblowing team has reasons to believe that the identity would be revealed,

- the whistleblowing team will, to a reasonable extent, inform the reporting person, no later than within three (3) months upon confirmation, of the actions to be taken with regard to the report and the reasons why, and

- where applicable, the whistleblowing team will inform if the identity of the reporting person needs to be provided to an authorized third party, except where such information would hinder the investigation.

The person subject to the report shall also receive information on the processing of their personal data with regard to the report, except where such information would hinder the investigation (if so, information shall instead be provided at the latest when measures are being taken).

External reporting

Reporting to national authorities
Except internal reporting, an employee may also decide to report externally to a designated authority's established whistleblowing channel, depending on the subjectmatter of the report. Such authorities have an obligation to provide an external channel for reporting of certain misconducts, where there is a public interest, see further details on how to report in Appendix A.

When reporting externally, it is the relevant authority who is responsible for receiving the report, provide necessary information and follow-up. A report may be shared with another relevant institution when needed.

The centralized external reporting channel in Sweden is provided by the Swedish Work Environment Authority (Sw. Arbetsmiljöverket). External reporting also includes protection from retaliation and covered by rules on confidentiality.

Reporting to institutions within the EU
Where the subject-matter of the report falls within the area of expertise of an EU institution, the employee may report directly to such institution. The right to receive protection is based on the same requirements as internal reporting, hence the reporting needs to be made in accordance with such guidelines as communicated therewith.

Reporting through media
An employee may also receive protection when reporting publicly, provided that:

- a report has been made through an external reporting channel, without being appropriately addressed or investigated, or no appropriate remedial action has been taken within the set time frame,
- where reporting publicly is evident in order to safeguard an obvious risk for breaches relating to the health and safety of people or the environment (for example due to serious criminal offences relating to financing or the environment), or
- when the employee has valid reasons to believe that they would suffer retaliation in connection with the external reporting.

A reporting person may also report to media in accordance with their constitutional rights.

Protection afforded by the Freedom of the Press Act, Fundamental Law on Freedom of Expression etc

A reporting person is always covered by the Freedom of the Press Act (Sw: Tryckfrihetsförordningen) which, subject to certain exceptions, declares the freedom of every Swedish citizen to publish their thoughts and communicate information on any subject) and the Fundamental Law on Freedom of Expression (Sw: Yttrandefrihetsgrundlagen) defined as a freedom to communicate information in speech, writing or image or in any other way and to express thoughts, opinions and feelings).

Reporting persons are also covered by the freedom of acquisition (meaning that the reporting person cannot be held responsible for acquiring information as long as it is obtained in good faith and where the person has reasons to believe that it is necessary in order to expose the misconduct) and prohibition of investigation (meaning that there is no right to investigate the identity behind a report).

Prohibition on further investigation and the right to report in publicly funded companies/organizations

The constitutional rights also include a right to remain anonymous. An authority is prohibited from further investigating the identity of the reporting person or take any action on retaliation where an employee has provided information based on the above-mentioned constitutional rights.

The same applies in private organizations which are publicly funded, part of the educational system, healthcare system or social services.

Appendices:

Appendix A

Appendix A – External reporting channels (in Sweden)
Authorities that are currently required to provide specific reporting channels (as of July, 17 2022) are the following (note that the list is not exhaustive and may evolve):

Swedish Work Environment Authority (Sw. Arbetsmiljöverket)
The Swedish Work Environment Authority is the supervisory authority for employers' handling of whistleblowing. The Swedish Work Environment Authority also has an external reporting channel for misconduct covered by EU legislation and by the Swedish Work Environment Authority's supervision, i.e. product safety and product compliance, that you have become aware of in a work-related context. Information on how to report can be found on the Swedish Work Environment Authority's website.

The Swedish National Board of Housing, Building and Planning (Sw. Boverket)
In Boverket's external channel, you can report misconduct in a work-related context that has to do with product safety and product compliance. It must also be an instance of misconduct that falls within the Boverket's supervisory responsibility. Information on how to report is available on the Boverket website. Here you will also find a direct link to the platform.

National Electrical Safety Board (Sw. Elsäkerhetsverket)
You can report serious irregularities such as illegal manufacture, import or distribution of products covered by the LVD, EMC, ATEX, Radio Equipment or Toys Directives, the Gas Appliances Regulation and the General Product Safety Directive.

Public Health Agency (Sw. Folkhälsomyndigheten)
The Public Health Agency of Sweden receives reports of tobacco-related abuses that fall under its supervision. Information on how to report can be found on the Public Health Agency's website.

Swedish Agency for Marine and Water Management (Sw. Havs- och vattenmyndigheten)
The Swedish Agency for Marine and Water Management receives notifications of irregularities detected in the area of responsibility of the Agency and concerning supervision or regulatory guidance in the field of environmental protection and economic matters such as public procurement.

Swedish Authority for Privacy Protection (Sw. Integritetsskyddsmyndigheten, IMY)
You can report to IMY if you have information that the person you work or have worked for, or are applying to work for, is not complying with the General Data Protection Regulation (GDPR) or additional rules, such as the Data Protection Act. Information on how to report can be found on the IMY website.

Inspectorate of Strategic Products (Sw. Inspektionen för strategiska produkter, ISP)
The ISP, as a competent authority, receives reports from persons who, in a work-related context, wish to provide information on violations falling within the ISP's remit under the Act. Information on how to report can be found here on the ISP website.

Swedish Competition Authority (Sw. Konkurrensverket)
If you discover a violation in the areas of competition and public procurement in a work-related context, you can report it to the Swedish Competition Authority in accordance with the Act. The violation may, for example, concern incorrect direct procurement, unauthorised price cooperation or contractual conditions that harm competition. Information on how to report can be found here on the Competition Authority's website.

Swedish Food Agency (Sw. Livsmedelsverket)
You can report irregularities concerning product safety/product compliance, environment radiation protection and nuclear safety, food, animal health and safety and data privacy that fall under the Swedish Food Agency's supervisory responsibility.

Swedish Medical Products Agency (Sw. Läkemedelsverket), MPA
If you discover irregularities in an activity that concerns the MPA's supervisory responsibility, you can report it to the MPA. Information on how to report can be found on the MPA's website.

County Administrative Boards (Sw. Länsstyrelserna)
The County Administrative Boards receive and handle reports of non-compliance in the areas of product safety/product compliance, environmental protection, prevention of money laundering and financing of terrorism. Each county has its own channel. Information on how to report can be found on the County Administrative Board's website.

Swedish Inspectorate of Auditors (Sw. Revisorsinspektionen)
You can report misconduct to the Inspectorate of Auditors if what someone does or what someone has failed to do is contrary to the provisions applicable to authorized and approved auditors and to registered audit firms. Information on how to report can be found on the Inspectorate's website.

The Swedish Tax Agency (Sw. Skatteverket)
The Tax Agency's external whistleblowing function only concerns certain abuses in the field of taxation covered by EU legislation, namely abuses in the financial interests of the EU in the field of taxation and internal market abuses in the field of corporate tax. For example, a company may have carried out or will carry out transactions aimed at circumventing or exploiting tax legislation in order to obtain a tax advantage. For example, it may involve transactions of a tax avoidance nature. In most cases, tax avoidance involves practices whereby a taxpayer carries out one or more transactions primarily for the purpose of obtaining or avoiding a tax effect, such as seeking a deduction for a false loss. Information on how to report can be found on the Swedish Tax Agency's website.

The Gaming Inspectorate (Sw. Spelinspektionen)
The Swedish Gaming Inspectorate is responsible for receiving whistleblowing reports concerning irregularities in the area of prevention of money laundering and financing of terrorism within the authority's supervisory area, i.e. gaming companies licensed in Sweden. Information on how to report can be found on the Spelinspektionen's website.

Swedish Economic Crime Authority (Sw. Ekobrottsmyndigheten)
The whistleblowing function of the Swedish Economic Crime Authority deals exclusively with misconduct affecting the EU's financial interests. These may include: fraud subsidy abuse certain customs offences certain VAT offences acts in breach of conditions for EU aid false certification in certain cases, corruption, double funding, etc. Information on how to report can be found on the website of the Swedish Economic Crime Authority.

The Swedish Estate Agents Inspectorate (Sw. Fastighetsmäklarinspektionen, FMI)
If you are connected to the broker industry, you can contact the FMI if you become aware that someone within a broker company is violating money laundering rules. Information on how to report can be found on the FMI website.

The Financial Supervisory Authority (Sw. Finansinspektionen, FI)
FI receives reports from persons who, in a work-related context, wish to provide FI with information about misconduct that is in the public interest. A report must relate to a concrete suspicion that a company or a private individual has violated a regulatory framework that falls under FI's supervisory responsibility.

Appendix A

The Health and Social Care Inspectorate (Sw. Inspektionen för Vård och Omsorg, IVO)
The area of responsibility in the field of public health which is covered by the authority's supervisory responsibility is blood, tissue and transplant activities. IVO is also responsible for malpractice in the area of privacy and personal data protection and network and information system (NIS) security, which falls under the Authority's supervisory responsibility. Information on how to report can be found on the IVO website.

The Swedish Chemicals Agency (Sw. Kemikalieinspektionen, Kemi)
You can report whistleblowing to Kemikalieinspektionen to report violations of certain chemicals legislation for which Kemi is the competent authority. An example of such misconduct is when a company imports toys containing unauthorized chemical products into Sweden. Information on how to report can be found on Kemi's website.

The Swedish Consumer Agency (Sw. Konsumentverket)
You can report complaints concerning product safety, public health and consumer protection that fall within the scope of the Consumer Agency's supervision, in accordance with legislation common to the EU Member States. Information on how to report can be found on the Consumer Agency's website.

Swedish Civil Contingencies Agency (Sw. Myndigheten för samhällsskydd och beredskap, MSB)
The Swedish Civil Contingencies Agency receives, follows up and provides feedback on reports of nonconformities in the area of product safety and product compliance that fall under the Swedish Civil Contingencies Agency's market surveillance responsibilities. Information on how to report can be found on the Swedish Civil Contingencies Agency website.

The Swedish Environmental Protection Agency (Sw. Naturvårdsverket)
You can notify PTS of serious irregularities or breaches of regulations in the areas of product safety and conformity, protection of privacy and personal data, or security of network and information systems. Information on how to report can be found on the PTS website.

The Swedish Post and Telecom Authority (Sw. Post- och telestyrelsen, PTS)
You can notify PTS of serious irregularities or breaches of regulations in the areas of product safety and conformity, protection of privacy and personal data, or security of network and information systems. Information on how to report can be found on the PTS website.

Government Offices of Sweden (Sw. Regeringskansliet)
Abuses relating to state aid can be reported to the Government Offices. Information on how to report can be found on the Government's website.

The Swedish Energy Agency (Sw. Statens energimyndighet)
The Swedish Energy Agency works to prevent corruption and irregularities. In case of suspicion of serious irregularities within the Swedish Energy Agency. More information on how to report can be found at: report.whistleb.com/sv/Energimyndigheten

Sweden's national accreditation body (Sw. Styrelsen för ackreditering och teknisk kontroll, SWEDAC)
Swedac's area of competence is misconduct in the field of product safety and product conformity that falls under Swedac's supervisory responsibility and that contravenes the directives to which the Whistleblowing Directive applies. More information on how to report can be found on Swedac's website.

Swedish Radiation Safety Authority (Sw. Strålsäkerhetsmyndigheten)
For those who want to safely report misconduct in a work-related context in the field of radiation protection and nuclear safety that falls under the regulatory responsibility of the Agency. Information on how to report can be found on the website of the Radiation Safety Authority.

Swedish Transport Agency (Sw. Transportstyrelsen)
If, in a work-related context, for example as an employee, you have such information that you have reasonable grounds to believe that your operator is in breach of EU law, you can, in certain cases, make a notification to the Swedish Transport Agency. Information on how to report can be found on the Swedish Transport Agency's website.

The Swedish Forest Agency (Sw. Skogsstyrelsen)
You can notify the Swedish Forest Agency of irregularities that fall under the Agency's supervisory responsibility. Information on how to report can be found on the Swedish Forest Agency's website.

Appendix B

Privacy policy
Regarding the processing of personal data within the whistleblowing channel IntegrityLog

This privacy policy describes how **Scandinavian Airlines System Denmark-Norway-Sweden**, a consortium established under the laws of Denmark, Norway and Sweden, having its principal office at Frösundaviks allé 1, 195 87 Stockholm, Sweden, (hereinafter "SAS", "we", "our" and "us") as the judicial person responsible for personal data processing in relation to you as an employee or former employee. This Privacy Policy is applicable for the whole SAS Group, regardless of which company you are employed at. Please see Attachment A to this Privacy Policy – Applicability of Privacy Policy, to understand the scope of this Policy.

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 policy.

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 dataprotectionofficer@sas.se

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 on their website, complylog.com

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

Personal data that we may process
- Name, telephone number, address, e-mail address of the whistleblower;
- 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);
- Names and contact details of any witnesses or other people involved in the case;
- Information on how notifications are made, processed, and communicated (including notification code and status);
- Other information provided by the notifier that contains personal data;
- Information about those who process notifications that come through the Channel, e.g., name, job title, email address, user ID.

Purpose for the processing
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.

Legal bases for the processing
- To fulfill our legal obligation (Article 6(1)(c) of the GDPR);
- Our legitimate interest in ensuring the legality and ethics of our operations (Article 6(1)(f) of the GDPR;
- 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.

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 are not authorized 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.

Appendix B

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.

Attachment A

– Applicability of Privacy Policy

SAS GROUP
Legal structure 2023, September 2023