ADAPTIVE **RECOGNITION**

Policy
on the internal whistleblowing system

Content

Policy
on the internal whistleblowing system

I. Objectives and scope of the present policy

The **ARH Informatics Company Ltd.** (registered seat: H-1123 Budapest, Alkotás street 41., company registration number: 01 10 044343, hereinafter: „**Company**") with regards to the provisions of Act XXV of 2023 on complaints, notifications of public interest and rules on reporting breaches (hereinafter: „**Act**"), shall establish and operate an internal breach reporting system (hereinafter: „**System**").

The present policy (hereinafter: „**Policy**") incorporates the applicable rules regarding the establishment and the operation of the System.

By creating this Policy and making it available at its registered office the Company intends to fulfil its obligation under Article 25 of the Act, i.e. to provide clear and easily accessible information on the operation of the System, the whistleblowing procedure, the protection of whistleblowers (hereinafter: „**Whistleblower**"), and the whistleblowing systems and procedures under the Act.

II. General rules on reporting breaches

1. Scope of the report – what is a breach which can be reported?

Through the System information about an unlawful or suspected unlawful act or omission or other breach can be reported.

The report shall be deemed lawful in the cases specified in Article 45 - 47 of the Act. This includes, inter alia, and as a general rule, where the Whistleblower has made the report through the System in accordance with the rules set out in the law and in the Policy, the Whistleblower has obtained the notified information in the context of his/her employment or other activities as defined in Section II.2 of the Policy and has reasonable grounds to believe that the notified information was true at the time of reporting it.

The design and operation of the System ensures the completeness, integrity and confidentiality of the information contained in the report and enables the permanent storage of the information contained in the report to allow for possible future investigations.

2. Persons entitled to file a report – who can be a Whistleblower?

Both employees and contractual partners of the Company, as well as other persons having a legal or relevant relationship with the Company as described below, are entitled to make a report through the System.

The following persons may make a report through the System:

- an employee of the Company; including persons whose employment relationship has been terminated; and persons for whom the procedure for the establishment of an employment relationship has been initiated (i.e. who have attended a job interview organised by the Company)
- any sole proprietor or sole proprietorship who has a contractual relationship with the Company, including persons whose contractual relationship has been terminated or for whom a procedure to establish such a relationship has been initiated;
- person with an ownership interest in the Company, and a member of the Company's administrative, management or supervisory body, including a non-executive director (in the case of a director, from the date of the invitation to hold such office or, failing this, from the date of the declaration of acceptance of the office);

- contractor, subcontractor, supplier or person under the supervision and control of a trustee who has or has had a contractual relationship with the Company, including those whose contractual relationship has been terminated or who have commenced the procedure for entering into a contractual relationship with the Company (i.e. including persons who have bid for a contract);
- trainees and volunteers of the Company (from the date of application to the Company for such positions), including persons who have ceased to hold such positions.

3. Protection of Whistleblowers

In accordance with the principles and values set out above, the Company encourages its employees and partners, as well as other persons entitled to make a report, to make a report in all cases of abuse, misconduct, illegal conduct (acts or omissions) or suspected misconduct of which they become aware.

The Company considers the protection of Whistleblowers to be of the utmost importance, and therefore it is mandatory to ensure that Whistleblowers acting in good faith are not subject to any discrimination, disadvantage or unfair treatment or negative consequences in connection with their report. The Whistleblower shall not be disadvantaged even if the report made in good faith proves to be unfounded during the investigation.
Pursuant to the Act, any adverse action (including, for example, termination, assignment of job duties, negative performance appraisal, reduction of salary) taken against the Whistleblower as a result of the lawful filing of a whistleblowing complaint and taken in connection with the legal relationship or relationship between the Company and the Whistleblower as set out in Section II.2 of the Policy shall be unlawful, even if it would otherwise be lawful.

When conducting investigations and reporting complaints, the Company will make every effort, through the design of the System, to treat the identity of the Whistleblower or the person with information in connection with the report as confidential as possible.

The System is designed in such a way that the personal data of the Whistleblower who discloses his or her identity and of the person concerned by the report or the person who has substantial information about the subject matter of the report cannot be disclosed to persons other than those authorised to do so.

Until the investigation is closed or formal proceeding is initiated, the persons investigating the report shall not share information about the content of the report and the person concerned

with any other department or employee of the Company except to the extent strictly necessary for the conduct of the investigation.

In case a report is lawfully made, the Whistleblower shall not be deemed to have breached any restriction on disclosure of a legally protected secret or any other legal restriction on disclosure of information and shall not be liable in respect of such report if the Whistleblower had reasonable grounds to believe that the report was necessary to disclose the circumstances to which it relates. Furthermore, where a report has been lawfully made, the Whistleblower shall not be liable for obtaining or accessing the information contained in the report, unless the Whistleblower has committed a criminal offence by obtaining or accessing the information. The Whistleblower shall not be held liable for lawfully making the report if he/she had reasonable grounds to believe that the report was necessary to disclose the circumstances to which it relates.

The protection granted to the Whistleblower also applies to anyone who assists the Whistleblower filing a lawful report in making the report, and also to the Whistleblower making a lawful report anonymously, if the Whistleblower is later identified and would be subject to adverse action.

III. Procedure of handling the reports

1. Procedure for making a report

The Whistleblower is entitled to make the report verbally or in writing. It is also possible to make a report without revealing the identity of the Whistleblower (i.e. anonymously), however, in this case, the identification of the Whistleblower may be necessary for a substantive investigation of the report.
The verbal report can be made by phone: +36 70 777 8096.

The operator of the System shall record the verbal report in writing by drawing up a complete and accurate protocol (with the possibility to check, correct and sign the document incorporating the report) and shall provide a copy to the Whistleblower.
Even when reporting verbally, it is necessary to refrain from reporting in bad faith. The opera-

tor of the System shall warn the Whistleblower of the legal consequences of reporting in bad faith and inform the Whistleblower of the applicable procedural rules and the confidentiality of any personal identification information provided. If the Whistleblower provides personal data during the making of the report, confidentiality will be ensured throughout the process.

The written report can be made by sending an e-mail to ceg@arh.hu with the necessary information for the report. Written report can also be made by sending a postal letter to ***H-1123 Budapest, Alkotás street 41. Hungary.***

The operator of the System shall send a confirmation of the written report within seven (7) calendar days of receipt of the report to the Whistleblower, at the same time informing her/him of the procedural and data management rules applicable according to the Act.

The operator of the System may, in the case of a non-anonymous report, request additional information or clarification of the information provided by the Whistleblower, in a manner appropriate to the time of the submission of the report, in order to allow for a substantive investigation of the report, by setting a reasonable deadline.

At the same time as making the report, the Whistleblower declares that, in making the report, she/he is acting in good faith and has reasonable grounds to believe that the information reported was true at the time of submitting the report.

2. Procedure for examining the content of the report

In all cases, the procedure for the examination of the content of the report shall be conducted in accordance with the provisions of the Policy and the applicable legislation, irrespective of the identity and position of the Whistleblower and the persons concerned by the report.

The System ensures that reports are investigated fairly, impartially and in accordance with ethical principles. Accordingly, the Company shall ensure, through the design and the operation of the System, that persons affected in any way by a report are treated fairly and equitably, with due regard for the presumption of innocence, and subject to the principle of proportionality in any action taken.

Handling a report without a substantive investigation

The substantive examination of the report can only be disregarded in the following cases:
- if the report was made by an unidentifiable Whistleblower,
- if the report was not made by a person entitled to make a report (as defined in point II.2 of the Policy),
- if the report is a repeated report by the same Whistleblower with the same content as the previous report,
- where the harm to the public interest or to an overriding private interest would not be proportionate to the restriction of the rights of the natural or legal person concerned by the report resulting from the investigation of the report (for example, the suspension of work required to investigate the report would not be proportionate to the reported act).

If no substantive examination of the report is carried out, the Whistleblower must be informed of the decision not to proceed and its reasons.

Substantive examination of a report

The operator of the System shall investigate the allegations contained in the report as soon as circumstances permit, but no later than 30 days from the date of the receipt. This time limit may be extended only in particularly justified cases, subject to simultaneous notification to the Whistleblower (including the expected date of the investigation and the reasons for the extension), for a maximum period of three months from the date of receipt.

During the investigation of the report:
- the relevance of the circumstances included in the report shall be assessed,
- appropriate measures must be taken to remedy the breach which is the subject of the report,
- where the report warrants the initiation of criminal procedure, arrangements should be made to bring charges.

The operator of the System shall inform the Whistleblower in writing of the results of the investigation and of the measures taken or planned.

3. Informing the person concerned by the report

The person concerned by the report shall be informed in detail about the report, his or her rights in relation to the processing of personal data and the rules applicable to the processing of his or her data when the investigation based on the report is initiated.

In exceptional and justified cases, the person concerned may be informed at a later stage than the initiation of the investigation, if immediate information would prevent the investigation of the report.

The person concerned by the report shall be given the opportunity by the operator of the System, in accordance with the requirement of due process, to express his/her legal opinion on the report, including through his/her legal representative, and to provide evidence in support of such opinion.

IV. Information relating to the system

1. Basic rules on data management in relation to reports

The personal data of the Whistleblower will be treated confidentially by the operator of the System, in accordance with the provisions of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter: „**Regulation**" or „**GDPR**").

Within the framework of the System, regarding
a) the Whistleblower,
b) the person whose conduct or omission gave rise to the report; and
c) the person who may have material information about the facts contained in the report, personal data which are indispensable for the investigation of the report may be processed solely for the purpose of investigating the report and remedying or stopping the conduct which is the subject of the report.

Personal data not covered by points a) to c) of this Section shall be deleted without delay from the data processed within the System.

The personal data of the Whistleblower – with the exception of the data of the Whistleblower who has provided manifestly bad faith or false information – may only be disclosed to the state body or authority competent to conduct the proceedings initiated on the basis of the report, if this state body or authority is entitled to process the data by law or if the Whistleblower has consented to the disclosure of his/her data. The personal data of the Whistlblower shall not be disclosed without his/her explicit consent.

If it has become apparent that the Whistleblower has, in bad faith, provided false data or information and

a) in this connection, circumstances suggesting that a criminal offence or irregularity has been committed have arisen, the personal data of the Whistleblower shall be handed over to the public body, authority or person entitled to conduct the proceedings,

(b) there are reasonable grounds to believe that he or she has caused unlawful harm or other legal damage to another person, his or her personal data shall be disclosed upon request to the public body, authority or person entitled to initiate or conduct the proceedings.

If the report relates to a natural person, in exercising his or her right to information and access under the provisions on the protection of personal data, the personal data of the person making the report may not be disclosed to the person requesting the information.

Data processed within the framework of the System may be transferred to a third country or to an international organisation only if the recipient of the transfer has given a legal undertaking to comply with the rules on notification set out in the Act and in compliance with the provisions on the protection of personal data.

The identity of the Whistleblower, the person concerned by the report or the person who may have substantial information about the facts contained in the report shall not be disclosed to any person other than the person entitled to know the personal data.

The notice on the processing of personal data processed in connection with the System is set out in Annex 1 to the present Policy.

2. Information on whistleblowing schemes and procedures under the Act

Under the Act, all employers who employ at least 50 persons under an employment relationship must set up an internal whistleblowing system.

Employers who employ at least 50 but not more than 249 persons under an employment relationship may jointly set up an internal whistleblowing system.

[1] Employer: who employs a natural person under an employment relationship.

[2] Employment relationship: any legal relationship in which an employee performs an activity for and under the direction of an employer for remuneration or for self-employment.

Irrespective of the number of employees, some employers are required to set up an internal whistleblowing system under the Act, such as credit institutions, financial service providers, auditors, trusts and headquarters service providers. If the employer is a public body, a local government or a fiscal organisation under their management or supervision, or an organisation or company owned or controlled by them, it is obliged to set up an internal whistleblowing system irrespective of the number of employees, subject to certain exceptions provided for by law. Certain public bodies (e.g. the Hungarian Competition Authority, the Public Procurement Authority, the Hungarian National Bank, the National Authority for Data Protection and Freedom of Information) are required to establish a separate whistleblowing system.

The internal whistleblowing system may be operated by an impartial person or department within the employer who has been appointed for this purpose. The system in case of employers of the private sector may be operated by a contracted whistleblower protection lawyer or an external organisation, subject to the relevant conflict of interest and impartiality rules. The whistleblower can make the report verbally or in writing and has 30 days to investigate it, which may be extended to a maximum of three (3) months in exceptional and justified cases.

In the case of a whistleblowing system to be set up by the employers covered by the Act, the general provisions set out in Sections II.1.-3. of the Policy shall apply accordingly to the whistleblower, the subject of report and the protection of whistleblowers.

Employers are required to provide clear and easily accessible information on the operation of the whistleblowing system, the procedure for reporting, and the whistleblowing systems and procedures under the Act.

V. Closing provisions

The present Policy shall enter into force on 15th January 2024
and shall remain in force until revoked.

Privacy notice

on the processing of personal data in the frame of the internal whistleblowing system

Introduction

ARH Informatics Company Ltd. (hereinafter: „**Company**") establishes and operates an internal whistleblowing system (hereinafter: „**System**") with the involvement of an external organisation in view of the provisions of Act XXV of 2023 on complaints, notifications of public interest and rules on reporting breaches (hereinafter:"**Act**"), thus the purposes and means of data management are jointly determined, and therefore they are considered joint controllers.

Through the System information about an unlawful or suspected unlawful act or omission or other breach can be reported.

The purpose of this Notice is to provide Data Subjects with information about the processing of their personal data within the framework of the System, which is indispensable for the investigation of the reports, the purpose and the legal basis of the processing, the identity and contact details of the controller, and basic information on the processing.

The purpose of the Policy is also to inform the Data Subjects:

- about their rights in relation to data processing concerning them,
- about who and how they can contact with their requests and questions concerning the data processing of their personal data, from whom they can obtain the requested information and how long will it take to obtain the information requested,
- if they consider that their rights have been infringed in connection with data processing, for example, if they have not been adequately informed about or do not agree with the data processing or if they consider that the processing of their personal data is unlawful, in this case, to whom they can turn with their complaint and from which body they can seek legal protection.

1. Name and contact details of the Data Controllers

Name: ARH Informatics Company Ltd.
Registered seat: H-1123 Budapest, Alkotás street 41.
E-mail: ceg@arh.hu
Name: Viktor Kertész

2. Basic provisions governing data processing

2.1. For the purposes of this Policy:
Personal data: any information relating to an identified or identifiable natural person („Data Subject"), such as any information about You or any other natural person, such as name, email address;
Controller: the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (See point 1.).

2.2 Controller is responsible for compliance with the following principles when processing your personal data:

a) process personal data lawfully, fairly and transparently in relation to the Data Subject („lawfulness, fairness and transparency");

b) collect personal data only for specified, explicit and legitimate purposes and does not process them in a way incompatible with those purposes. („purpose limitation")

c) the personal data processed are adequate, relevant and limited to what is necessary for the purposes for which they are processed („data minimisation");

d) keep the personal data accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay („accuracy")

e) store the personal data in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed; („storage limitation");

f) a process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures („integrity and confidentiality").

2.3. Our data management activities are carried out in accordance with the applicable European Union and national legislation in force, in particular:

a) Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); (The EU General Data Protection Regulation), (hereinafter: GDPR),

b) Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information.

3. Identification of Data Subjects, scope of personal data processed, purpose of processing, legal basis

Information about unlawful or suspected unlawful acts or omissions, or other breach, may be reported to the System. The Whistleblower may make the report in writing or verbally. The System will process the personal data of the Whistleblower and the personal data of the person whose conduct or omission gave rise to the report and who has relevant information in relation to the report (all of whom may be considered as Data Subjects). All other personal data not covered by the foregoing will be deleted from the System without delay.

Scope of data processed:

- the personal data of the Whistleblower which are indispensable for the investigation of the report (such as the name of the Whistleblower (if not anonymous); e-mail address (if the report is not verbal));
- personal data of the person whose conduct or omission gave rise to the report, which are indispensable for the investigation of the report;
- the personal data of the person who is indispensable for the investigation of the report and who may have material information about the content of the report.

Personal data not covered by the above shall be deleted immediately from the data processed within the System.

Legal basis for processing: to comply with a legal obligation (Article 6(1)(c) GDPR).We are obliged to investigate and process the notification according to the provisions of the Act.

Purpose of processing: to ensure that the report can be made; to investigate the report and to take the necessary measures to remedy or eliminate the conduct that is the subject of the report; to send the whistleblower an acknowledgement of receipt of the report; to contact the whistleblower, to complete or clarify the report, to clarify the facts and to provide additional information in order to be able to investigate the report; to provide information on the outcome of the investigation of the report.

Duration of data processing: we will keep the data until the purpose specified above has been achieved (until the investigation of the report has been closed). If the investigation reveals that the report is unfounded or that no further action is necessary, the Data Controller will delete the data relating to the report within 60 days of the end of the investigation. Where action is taken on the basis of the investigation, including legal proceedings or disciplinary action against the person making the report, the Data Controller shall keep the data relating to the report until the proceedings based on the report have been finally closed.

The personal data of the whistleblower may only be transferred to the public body or authority competent to conduct the procedure initiated on the basis of the report, if such public body or authority is entitled to process the data by law or if the whistleblower has consented to the transfer of the data. Personal data of the whistleblower shall not be disclosed without his/her consent. Where it has become apparent that the whistleblower has communicated false data or information in bad faith, his or her personal data shall be disclosed, upon request, to the body or person entitled to initiate or conduct the relevant proceedings.

4. Access to data and data security measures

The Company uses the assistance of an external organisation for the operation of the whistleblowing system. The external entity and the Data Controller act as joint data controllers.

Data processed within the framework of the System may be transferred to a third country or to an international organisation only if the recipient of the transfer has given a legal undertaking to comply with the rules on notification set out in the Act and in compliance with the provisions on the protection of personal data.

The Data Controller will take all reasonable technical and organisational measures to protect your personal data against, including but not limited to, unauthorised access or unauthorised alteration. We ensure that your personal data is protected at all times from unauthorised access.

We may be approached by a court, prosecutor's office, investigating authority, infringement authority, administrative authority, the National Authority for Data Protection and Freedom of Information, and other authority(ies) authorised by law to transfer or transmit personal data in connection with data processing.
In such cases, we will only disclose information that we are legally required to disclose and to the extent that it is strictly necessary to fulfil the request.
.

5. Rights of the Data Subject in relation to data processing, legal remedies

5.1. The Data Subject may request (using the contact details indicated in point 1.)

a) information on the processing of his/her personal data,
b) rectification of his/her personal data,
c) restriction of the processing of his/her personal data (in specific cases),
d) erasure of personal data (except for processing required by law).

At the request of the Data Subject, the Data Controller shall

· Provide information as to whether or not his or her personal data are being processed, if so, including the purposes of the processing, the categories of personal data concerned by the processing, the recipients of the data in the event of transfer, the duration of the processing, the rights of the Data Subject, his or her rights of remedy, and, where the data do not originate from the Data Subject, the source of the data.

· Provide the information in writing and in an understandable form within the shortest possible time from the date of the request, but not later than 1 month from the date of receipt of the request. This information shall be free of charge. If the Data Controller can prove that the Data Subject's request is unfounded or excessive, the Data Controller may charge a fee or reject the request.

· If the Data Subject requests a copy of the personal data that are the subject of the processing, the Data Controller shall provide it. For additional copies requested by the Data Subject, the Data Controller may charge a reasonable fee based on administrative costs.

· The Data Controller shall, at the request of the Data Subject, correct inaccurate personal data relating to the Data Subject without undue delay or supplement incomplete personal data on the basis of a supplementary declaration.

Data Controller

· erases personal data where the processing is unlawful, where the purpose of the processing has ceased, where the personal data must be erased in order to comply with a legal obligation to which the Data Controller is subject, where the Data Subject withdraws his or her consent to the processing and there is no other legal basis for the processing.

· restricts processing at the request of the Data Subject where the Data Subject contests the accuracy of the personal data or where the processing is unlawful and the Data Subject opposes the erasure of the data, where the processing of personal data is no longer necessary for the purposes of the processing but is necessary for the exercise of a legal claim by the Data Subject, or where the Data Subject has objected to the processing. In such a case, the Data Controller may process the personal data, except for storage, only with the consent of the Data Subject or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or of an important public interest.

Upon request of the Data Subject for rectification, erasure or restriction of personal data, the Data Controller shall inform the Data Subject of the action taken in response to the request without undue delay and in any event within one month of receipt of the request. If the Data Controller does not take action on the Data Subject's request, it shall inform the Data Subject of the reasons for the lack of action and of the possibility to lodge a complaint with the supervisory authority and to exercise his or her right of judicial remedy within 1 month of receipt of the request at the latest.

The Data Controller shall notify the Data Subject of the rectification, restriction of processing and erasure.

5.2. Procedures for exercising rights in relation to data processing

The Data Controller will inform you of the action taken on your request pursuant to Articles 15 to 22 of the GDPR within one month of receipt of your request at the latest, which may be extended by two months if necessary (taking into account the complexity of the request and the number of requests, pursuant to Article 12 (3) of the GDPR).
Any extension of the deadline will be notified within the time limit set for the procedure, stating the reason for the extension.

5.3. Legal remedies

If you wish to lodge a complaint about the processing, you should first send it to the contact details provided in this notice, which will be investigated by the Data Controller immediately upon receipt, but no later than 1 month, and the complainant will be informed of the outcome of the investigation.

Complaint

The Data Subject may lodge a complaint with the National Authority for Data Protection and Freedom of Information if he or she considers that a breach of rights has occurred in relation to the processing of personal data concerning him or her.

Where to lodge a complaint:

National Authority for Data Protection and Freedom of Information
Address: H-1055 Budapest Falk Miksa u. 9-11., 1363 Budapest, Pf.9.
Fax: +361-391-1410,
E-mail: ugyfelszolgalat@naih.hu

Right to judicial remedy
The Data Subject shall have the right to judicial remedy if he or she considers that the data controller has not processed personal data relating to him or her in accordance with the rules of the Regulation and that his or her rights have been adversely affected as a result.
The action may be brought before the courts for the place of residence or domicile of the Data Subject.

Right to compensation, damages
If the controller causes damage by infringing the law on data processing, the controller must compensate the damage.
If the Data Subject's right to privacy is also infringed by processing in breach of the rules, he or she is entitled to damages.

If you have any questions or comments about this Notice, please contact us at the telephone number or e-mail address indicated in the Introduction to this Notice or by letter to our postal address.

The present Policy is published in English and Hungarian, in case of any discrepancy between the two versions, the Hungarian version shall prevail.

Effective from 15th January 2024