Short Public Report

Recertification No. 01

1. Name and version of the IT-based service:

SpeakUp System® function as provided in 2018-09-05

2. Provider of the IT-based service:

Company Name: People Intouch B.V (Hereinafter PIT)

Address: Olympisch Stadion 6, 1076 DE Amsterdam, Netherlands

Contact Person: Maurice Canisius

mauricecanisius@peopleintouch.nl

M +31 6 11 82 27 78 T +31 20 673 10 35

3. Time frame of evaluation:

2018-02-18 -- 2018-09-05

5. EuroPriSe Expert who evaluated the IT-based service:

Name of the Legal Expert: Johan Dahlsjö

Address of the Legal Expert: Götabergsgatan 20

SE-411 34 Gothenburg, Sweden

johan.dahlsjo@jpadvokatfirma.se

Name of the Technical Expert: Johan Dahlsjö

Address of the Technical Expert: Götabergsgatan 20

SE-411 34 Gothenburg, Sweden

johan.dahlsjo@jpadvokatfirma.se

6. Certification Authority:

Name: EuroPriSe Certification Authority

Address: Joseph-Schumpeter-Allee 25

53227 Bonn

Germany

eMail: contact@european-privacy-seal.eu

7. Specification of Target of Evaluation (ToE):

The standard set-up of the processor service SpeakUp provided by PIT (the SpeakUp System®).

The SpeakUp System® includes:

- Phone reporting functionality for persons reporting an irregularity

- Web reporting functionality for persons reporting an irregularity

- Back office translations and quality checks

- A case management module supporting receiving and handling of the message by the company designated officers

- Supporting information with standard templates and instructions

- Interfaces to third parties

Components of the service that are not part of the ToE:

- Unique client specific customizations

- Hardware and software used by customers, IT-providers and translators

- Third party networks

8. General description of the IT-based service:

The SpeakUp System® is a processor service that enables multilingual communication between designated officers at the clients and people reporting serious irregularities (messengers). For companies the SpeakUp System® serves as a key early warning system, as part of their broader compliance, ethics or sustainability program. In the past years, legislation (anti-corruption legislation as well as whistleblowing protection legislation) is pushing companies for a more secure and low-barrier reporting system.

The SpeakUp System® has been designed according to the strong belief of PIT, that an (anonymous) internal reporting system should be positioned as a last resort tool. This means that the organisational culture and policy should encourage and facilitate that employees first report via regular communication channels, like line management. This is also at the core of the implementation and awareness advice of PIT.

Web and Free Phone reporting

The messengers may report using a free phone number or a web form. This support cultural or personal communication preferences of the messengers, and may lower the barrier to report. For the clients, receiving the information, and starting to communicate, the selected communication means of the messenger does not make any difference; web and phone are integrated in one database, and can be managed from one overview.

Multilingual and Translations

For both reporting possibilities, the messenger can choose to receive all the information in his/her native language and to communicate in his/her native language. Efficient dialogue can be established due to the fact that immediate translations, transcriptions and recordings are part of the basic process. Furthermore, this crucial element of translations enables multinational companies to establish one central expertise centre for handling these messages, with independent professionals understanding also the importance of data protection. The SpeakUp System® includes an automated flow that facilitates a secured translation process. This currently runs for 75+ languages and the SpeakUp System is set up in 200+ countries.

Case Management Module

The SpeakUp System® has a case management module supporting the receiving and handling of the message by company designated officers. The case management module is not accessible for People Intouch. The case management module, helps clients to manage reports and store all investigation data on the secured servers.

9. Transnational issues:

The SpeakUp System® is web-based and distributed to users worldwide. However, the software and all data entered into the system is stored on servers in the Netherlands. Service operators, system administrators and translators are all located within the EEA or countries defined by the EU commission to have adequate protection of personal data.

PIT advices the Clients to implement additional safeguards to ensure that any transfer outside the EEA comply with applicable legal requirements.

10. Tools used by the manufacturer of the IT product / provider of the IT-based service:

None

11. Edition of EuroPriSe Criteria used for the evaluation:

Version of January 2017.

12. Modifications / Amendments of the IT-based service since the last (re)certification

A new Data Protection Officer with a legal background and a good knowledge of data protection legislation has been appointed.

The information package provided to the clients of the SpeakUp System® has been updated with new and improved templates as well as guidance supporting a GDPR compliant implementation.

The privacy statement for the SpeakUp System is updated.

Minor security improvements is made in the form of ongoing security updates.

13. Changes in the legal and/or technical situation

The General Data Protection Regulation (EU) 2016/679 (“GDPR”) was adopted 14 April 2016 and is enforceable from 25 May 2018. It replaces the Data Protection Directive 95/46/EC and has direct effect in the member states thus replacing all national legislation implementing the Data Protection Directive 95/46/EC.

New relevant opinions and guidelines based on GDPR has been published by the former EU expert group Article 29 Working Party:

- Opinion 2/2017 on data processing at work (wp249)
- Guidelines on Consent under Regulation 2016/679 (wp259rev.01)
- Guidelines on the Lead Supervisory Authority (wp244rev.01)
- Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)
- Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01)
- Guidelines on the right to "data portability" (wp242rev.01)
- Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)
- Guidelines on transparency under Regulation 2016/679 (wp260rev.01)

The Dutch Personal Data Protection Act is replaced by the GDPR and a Draft Implementation Act has been published for consultation but is not adopted yet.

14. Evaluation results:

The SpeakUp System® supports a legally compliant implementation of a whistle blower scheme (in all essential respects in accordance with the guidance "Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime", (hereinafter WP 117), published by the Article 29 Data Protection Working Party.

Purpose-specification and – limitation

The SpeakUp System® is a processor service designed to facilitate the clients scheme for reporting of serious financial and integrity irregularities and the management of reported messages. The SpeakUp System® is not designed or intended for any other purpose.

Data Avoidance and Minimisation

Messengers have the possibility to leave messages anonymous or under a pseudonym. The clients (the controllers) are supported by PIT with information to help messengers, who choose to be anonymous, not to reveal his/her identity by mistake. All personal data are deleted or anonymised within limited retention periods and no personal data of any kind is retained more than 60 days after a case is closed by the client.

The SpeakUp System® facilitates that access to personal data is set on a high level of granularity and reminds the clients to finalize open cases and observe adopted retention policies. The case management module enables the client users to set their own reminders to ensure that cases are managed and closed in a timely manner.

A Privacy Statement informs messenger that the service is not intended for sensitive personal data.

Data quality

The SpeakUp System® is designed to let messengers leave messages in their own language. A communication can be established between the messengers and client users, even if the messenger chooses to be anonymous. Wrongful statements and misunderstandings can thus be corrected before any investigation is started.

Transparency

The clients are supported by an extensive package of templates, manuals, leaflets and other documents describing the service and how to set up a legally compliant whistleblowing scheme. The information reflects GDPR, the guidance outlined in the policy paper WP 117, practical hints and detailed information about several aspects of the service.

The client users are informed about how to use the system via audio-visual tutorials accessible within the system. At the footer of every system webpage a privacy statement is available that provide client users, translators and system operators basic information about the processing of personal data when the service is used.

Legal basis

PIT is processing data on behalf of the clients and is in the sense of article 4 (8) of GDPR, a processor. A template data processing agreement, meeting all legal requirements, is used between PIT and its clients to establish these roles.

The main legal basis regarding whistleblowing schemes is balance of interests in accordance with article 6 (f) of GDPR.

For some clients the implementation of a whistleblowing scheme is necessary for compliance with a legal obligation in the sense of Article 6 (c) GDPR.

The processing within the SpeakUp System includes processing of employees' personal data in the employment context and depending on where the clients

are established applicable member state law and collective agreements may provide for specific rules.

Sensitive personal data may under certain circumstances be permitted according to Article 9 (2) (f) of GDPR, if the processing is necessary for the establishment, exercise or defence of legal claims.

The SpeakUp System® is not an electronic communications service in the sense of Article 2(c) of Directive 2002/21/EC and the service does not make use of cookies or processes personal data for unsolicited direct marketing. Thus, the requirements of Directive 2002/58/EC are not applicable to the SpeakUp System®.

Security

The information security regarding PIT and the security surrounding the SpeakUp System® follows strict documented processes. A written security policy based on ISO/ICE 27002 and COBIT Control framework is approved and adopted by PIT Management. The security policy sets out relevant security objectives inclusive rules and measures to pursue the objectives. PIT uses a structured framework for risk analysis.

The overall information security is recurrently by a well repudiated information security firm performing penetration tests.

All communication with the SpeakUp System® is protected by SSL/TLS encryption (HTTPS) and all data in the system is encrypted and stored on servers at high security data centres within the Netherlands.

All obsolete storage media is sanitised and securely destroyed under the direct supervision of PIT.

All new PIT employees and contractors must attend a special on-boarding program before they are assigned any tasks involving any form of processing of personal data. They also undertake to abide to strict integrity and confidentiality rules in writing. Mandatory training regarding privacy, security and confidentiality is performed within defined intervals.

PIT use special software for system monitoring and intrusion detection and have a well-defined process to be followed in case of any incident (e.g. a personal data breach).

The processors (the IT-supplier and the Translator Agencies) are closely monitored by PIT and bound by written processor agreements covering all necessary issues.

Data subjects rights

The clients are responsible as controllers to inform the persons who may be subject of a message, who leave a message, who receive and manage a message.

PIT provides the clients with information and templates to support proper handling of data subjects' rights under GDPR. The primary contact point supporting the clients when data subjects exercise their rights is the Data Protection Officer.

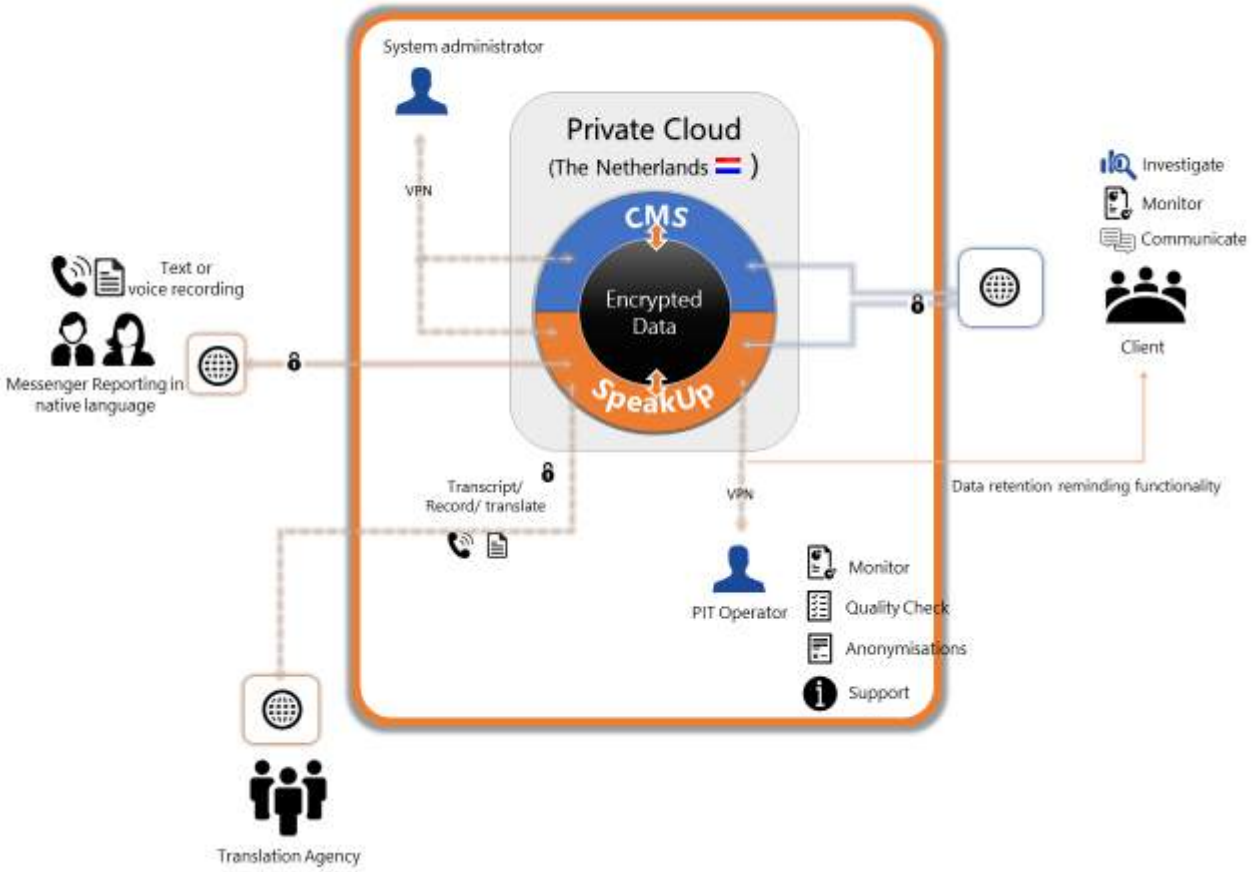
The clients are provided a possibility to publish customized information for messengers in the SpeakUp System®. A generic privacy statement addressing all system users is available in the footer of the system web pages. In addition client users are informed via a section in the manual of the SpeakUp System®.

Regarding the right to access, all personal data in the SpeakUp System® can be retrieved via a manual process in order to comply timely and effectively with any access request. All personal data in the SpeakUp System® can also be corrected via a manual process.

Regarding the right to rectify and erasure, personal data within the case management module can be selectively corrected or erased by client users. PIT can further correct or erase any data in the SpeakUp System® on behalf of the clients via a manual process. There is no personal data transferred from the SpeakUp System® to any third parties that needs be informed of any request from data subjects to rectify or erase data.

Regarding restriction of processing the clients can manually use the free-form text fields to mark a case as restricted and remove access rights to the case information to an absolute minimum.

15. Data flow:



16. Privacy-enhancing functionalities:

The clients of the SpeakUp System® are provided an extensive information package with new and improved templates and guidance supporting a GDPR compliant implementation.

The SpeakUp System® has functionality supporting client users to manage and close investigations in a timely manner and observe adopted retention policies.

Access rights can be set with high granularity which allows access to be set in accordance with a strict need-to know principle. Access can be restricted both in terms of content and predetermined time intervals.

A Data Protection officer with a legal background and good knowledge of data protection legislation is appointed.

17. Issues demanding special user attention:
    Not applicable

18. Compensation of weaknesses:
    Not applicable.

19. Decision table on relevant requirements:

EuroPriSe Requirement	***Decision***	***Remarks***
Data Avoidance and Minimisation	Excellent/ Adequate	Retention, and internal data disclosure, of personal data is limited to the extent necessary to provide the SpeakUp System®. Clients and messengers are advised that sensitive personal data shall be avoided when using the SpeakUp System®. Clients are supported by PIT with information to help messengers, who choose to be anonymous, to leave the message anonymous or under a pseudonym.
Transparency	Excellent	The clients using the SpeakUp System® are provided an extensive information package with templates, audio-visual tutorials. At the footer of every system webpage a privacy statement is available providing information about the processing of personal data when the service is used.
Technical-Organisational Measures	Excellent/ Adequate	The information security regarding PIT and the SpeakUp System® follows strict documented processes.

		The information security is reviewed periodically by independent third party experts with different competences. All obsolete storage media is sanitised and securely destroyed under the direct supervision of PIT. All message data is stored on physical servers in highly secured data centres in the Netherlands.
Data Subjects' Rights	Adequate	PIT provides the clients with information and templates to support proper handling of data subjects' rights under GDPR. The primary contact point supporting the clients when data subjects exercise their rights is the Data Protection Officer. PIT have processes to support clients regarding the data subjects' rights of access, rectification, restriction, erasure, objection and information of a personal data breach. The SpeakUp System® has functionality that can be used to support the data subjects' rights of restriction, rectification and erasure.

Experts' Statement

We affirm that the above-named IT-based service has been evaluated according to the EuroPriSe Criteria, Rules and Principles and that the findings as described above are the result of this evaluation.

Gothenburg, 10 September 2018

Place, date	Johan Dahlsjö	Signature of Legal Expert

Gothenburg, 10 September 2018

Place, date	Johan Dahlsjö	Signature of Technical Expert

Recertification Result

The above-named IT-based service passed the EuroPriSe evaluation.

It is certified that the above-named IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection.

Place, Date	Name of Certification Authority	Signature