

Data Privacy Impact Assessment – Template Short form

1 The need for a data privacy impact assessment (DPIA)

The aim

Briefly explain the context which requires the DPIA to be completed – what is the project, data sharing arrangement, provision of or change in services?

Eviosys has implemented a whistleblowing scheme for employees and certain outside or occasional collaborators to report violations. As recommended by the CNIL, the data processing resulting thereof should give rise to a DPIA insofar as it concerns employees considered as vulnerable persons and may give rise to the collection of sensitive data.

2 Describe the processing

The data subject (individual)

The information that will be handled relates to:

☐ our customers (including potential customer / website user)
☒ our employees ☐ our suppliers Other - *Outside or occasional collaborators (e.g., consultants) and potentially customers or suppliers if they are related issues reported pertaining to such persons.*

Does the information relate to ☒ vulnerable individuals or ☐ children?

Other - *The concerned persons would be employees (which are not necessarily vulnerable individuals depending on the issue at hand).*

The personal data / information

The information includes:

☒ name ☒ email (including work email) ☒ telephone number ☒ address ☐ payment details
☐ bank account numbers ☐ employee ID ☐ location data ☐ online identifiers ☐ facial recognition (CCTV) Other - *Other data may be collected depending on the facts reported (such as location data) and professional information.*

The information includes **special category of personal data** relating to ☐ race ☐ ethnicity ☐ sex life or sexual orientation ☐ political belief ☐ religious or philosophical beliefs ☐ trade union membership ☐ genetic information (including biometric data) ☐ mental or physical health or ☐ criminal offence *Normally, no sensitive data should be collected during the investigation, except if disclosed by the whistleblower or related to the scope of the reporting and disclosed during the investigation.*

The processing / handling of personal data

The term "processing" includes (but is not limited to) transferring, handling, recording, transmitting, hosting, storing, viewing, amending, destroying or otherwise using data. Consider including a

description of the data flow from start to finish. How will it be collected, used, stored, deleted? Where does the data come from? Is it shared?

The data will be collected following an alert received by Eviosys internally or via its Hotline provider when it is put in place. It is used to assess whether the facts alleged are accurate and verified, whether sanctions and/or other measures need to be implemented to cease the misconduct. It will be stored with restricted access on Eviosys's IT system and/or on the Hotline's platform also with restricted access. It will be shared with limited Eviosys employees in the legal team in charge of compliance, plant manager, audit, legal and HR, as well as certain external providers (legal, auditors), where required. If the alert is not admissible, the data will be deleted. If it gives rise to an investigation, documents and data collected during the investigation will be archived by the Compliance Officer. If there is no follow-up after the investigation, the data will be destroyed or anonymized within two months. If there are sanctions or legal proceedings, the data will be kept until the end of such proceedings and thereafter destroyed or anonymized, except for the information in the reporting register.

The purposes of the processing

Explain what we want to achieve by entering into this project / sharing data / changing the services in this way. What are the benefits to our business? What are the consequences to individuals?

Eviosys wants to investigate on the facts reported and take any required measures (such as the reinforcement of audit measures) and/or sanctions to prevent further wrongdoing and ensure compliance with policies. For individuals, the consequences may be potential sanctions, but the proper disciplinary procedure will be followed, the investigation will be impartial and neutral, the whistleblower and targeted person's identity will not be disclosed, except within the investigation team. The whistleblower will be protected against retaliation.

Third party access

Who else will have access to the data? What third parties are receiving the information?

The hotline provider may have access, as well as outside legal counsel, statutory auditors, public authorities where strictly necessary. Some of the data may also be sent to Eviosys' headquarters in Switzerland.

3 Considerations

Transparency

Consider the nature of your relationship with the individuals – what do they expect you to do with the information? Would they expect their data to be used this way? How much control will they have?

Most of the individuals concerned will be employees. They would expect that this data be kept confidentially at least during the investigation until its conclusion. They will have been informed prior about the rules pertaining to how Eviosys handles whistleblowing alerts. They can exercise their right of access. The identity of the whistleblower and targeted person will be protected.

Initial concerns

Are there previous concerns to take into account – security concerns, issues with the incumbent provider, etc. Is this a novel / bespoke system / handling of data?

This data is highly confidential and access rights will be limited on a need to know basis. Eviosys has chosen a Hotline provider offering sufficient security guarantees. Insofar as certain limited data may be transferred to the US, Eviosys has also entered into Standard Contractual Clauses to protect such data transfer.

Expert / stakeholder input

Include expert input – what is the development of technology in this field? Is there a current public shift in opinion in relation to this type of processing? Consider internal input as well as that from, for example, the supplier.

Rules for this type of processing are defined and set out with recommendations from the CNIL which Eviosys complies with. The hotline that will be chosen by Eviosys will need to provide for strict security and organizational measures and will enable Eviosys to define restricted access to the data collected and processed.

4 Assess necessity and proportionality

Lawful basis for processing

The reason that we can use personal data in this way:

☐ consent from individual ☐ necessary due to contract with individual ☒ necessary due to legal obligation (e.g. tax or regulatory obligation) ☐ vital interest of individual ☐ public interest / official authority ☒ legitimate interest which is not overridden by rights and freedom of the individual

Legitimate interest only insofar as the facts reported fall outside of applicable law (e.g., other than harassment or anti-bribery laws).

In addition to the reason above, the reason that we can use **special categories of personal data** (as indicated above) in this way:

☐ explicit consent from individual ☐ employment law, social security or social protection law ☐ vital interest of individual ☐ political, philosophical, religious or trade union charity ☐ personal data made public by individual ☒ establishment, exercise or defence of legal claims / courts acting in judicial capacity ☐ provision of health or social care, treatment or management ☐ public interest in public health ☐ archiving purposes in public interest, scientific or historical research / statistical purposes

Fit for purpose

How does the use of data in this way achieve the aim? Is there another way to achieve the same goal?

There is no other way to achieve the goal of processing the facts reported, investigating them so as to conclude on their existence and taking sanctions or measures to stop or prevent future wrongdoings.

Processing review

How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

See above. The data collected will be strictly limited to what is necessary to check the facts. Data quality and data minimisation will be taken into account. Individuals are informed prior to their alert of their possibility to report facts, their rights and protections. Concerned individuals will be also informed of this at the off-set of the investigation, when they report or are questioned. The whistleblower will be informed of the end of the investigation and of any follow-up. Eviosys will have entered into an agreement with processors providing for the GDPR processor obligations and reinforced confidentiality. If there are any international transfers outside of the EEA, they will be protected by sufficient safeguards, such as the SCCs.

5 Risks to individual's rights and freedoms

Risk	How does this processing impact the rights and freedoms of individuals?	Likelihood of harm	Severity of harm if occurred	Overall risk
A	Risk of violation of confidentiality and disclosure of identity of whistleblower	Possible	Significant	Low
B	Rights of defence of targeted person	Remote	Significant	Low

6 Measures to reduce risk



Consider additional measures you could take to reduce or eliminate risks identified as medium- or high-risk in section 5.

Risk	Measures to reduce or eliminate risk	Effect on risk	Remaining risk	Sufficiently mitigated?*
[5A]	Strict rules on the obligation not to disclose identity, limited and restricted access to information by persons subject to reinforced confidentiality provisions, no retaliation against whistleblower in good faith	Reduced	Low	Yes
[5B]	Strict rules on the obligation not to disclose identity, information of the targeted person on the alert (even if with slight delay to preserve evidence) and in most cases, interview during the investigation, compliance	Accepted	Low	Yes

Risk	Measures to reduce or eliminate risk	Effect on risk	Remaining risk	Sufficiently mitigated?*
	with legal disciplinary procedures			

7 Sign off and record outcomes

7.1 Sign off

Item	Name/date	Notes
Measures in section 6 approved by 	Juliana Castillo, Assistant General Counsel 3 February 2022	Ensure that actions are integrated into whistleblowing scheme which is currently being updated
Remaining risk approved by 	Laurent Watteaux, Chief Administrative Officer 3 February 2022	No residual high risk, therefore no need to consult supervisory authority before going ahead

7.2 Expert advice

Additional advice sought	Yes/No
Assistance of legal counsel (Addleshaw Goddard on compliance, section 6 measures and whether processing can proceed.	Yes
Was this advice followed?	Yes / No
If no, why? Include details as to who overruled the advice.	Yes

7.3 Ongoing review

This DPIA will be kept under review by	Juliana Castillo
--	------------------