whistlelink

Privacy Impact Assessment (“PIA”)

Introduction

If a processing of personal data is likely to result in a high risk to individual’s rights and freedoms, the Controller shall assess the impact of the processing on the protection of personal data according to Article 35 of the General Data Protection Regulation (“**GDPR**”). The PIA shall describe the risks and the measures taken to reduce these risks.

A PIA shall be carried out at as early as is practicable when a risk processing is to be performed, even if parts of the processing are still unknown. The assessment shall be performed by a person or a group of persons with significant insight in the processing (preferably the data protection officer if such has been designated) but not by the person who has the main responsibility for the processing. If the processing is carried out in whole or in part by a processor, the processor should participate in the PIA and provide the necessary information.

This PIA consists of:

1. A PIA-record to be completed with the relevant factors;
2. instructions for completing the PIA-record in eight steps; and
3. an overview of measures that are to be taken.

1. PIA-record

No.	1. The processing	2. Necessity and proportionality	3. Risk	4. Vulnerability	5.Measure(s)	6. Have the following parties been consulted?	7. Risk after the measure(s)	8. Is consultation with the supervisory authority required?
1.	Receiving whistleblowing information in Whistlelink	Mandatory under whistleblowing legislation	Risk that intentionally false, or otherwise incorrect information is reported in the system, meaning that incorrect personal data being processed.	High	It is always recommended that an initial screening av incoming reports are conducted by an appointed person knowledgeable in the system and the established processes around whistleblowing	Other party Data protection specialists at law firm	Accepted	No

2.	Submitting whistleblowing report	Mandatory under whistleblowing legislation	Risk that the company and/or Whistlelink personell identify anonymuous whistleblower in violation of internal rules and procedures	High	Technical measures in order to make it extremely difficult to access such information, including: There is no connection to the whistleblowers e-mail address, phone or any other contact details. It´s not mandatory to fill any contact details for the whistleblower. It´s possible for the client to add Intake Management from a third party and request that the third party remove any details of the whistleblower, if the whistleblower anyway have left details in the report. Functionality implemented to remove metadata in files.	Other party Indicate other party Data Protection specialists at law firm	Accepted	No

3.	Sending message to the whistleblower	Mandatory under whistleblowing legislation	Risk that some else than the whistleblower get access to the message.	High	When the whistleblower submit the report, the whistleblower get a unique case number and verification code, which is needed to access messages from the company.	Who has been consulted? Data Protection specialists at law firm.	Accepted	No
4.	Assigning the case to a case handler.	Necessary to have the relevant case handlers to handle each specific case.	Describe the risk Risk that someone else then the decided case handler gets access to the case.	High	User access functionality, where the owner or administrator over the account has to fill e-mail address and phone number of each added case handler. Two factor authentication functionality, possible for each user to add. Logging of each action from each user. Time limitations for using the system and being inactive.	Who has been consulted? Data Protection specialists at law firm.	Accepted	No

5.	Assigning the case to a third party, for example law firm or other investigator	Necessary to have the relevant experts to handle each specific case.	Describe the risk Risk that someone else then the decided person at the third party gets access to the case.	High	User access functionality, where the owner or administrator over the account has to fill e-mail address and phone number of each added case handler. Two factor authentication functionality, possible for each user to add. Logging of each action from each user. Time limitations for using the system and being inactive.	Who has been consulted? Data Protection specialists at law firm	Accepted	No
6.	Writing notes in the case	Necessary to have the information connected to the case in the system.	Describe the risk Risk that someone else then the decided persons gets access to the case.	High	User access functionality, where the owner or administrator over the account has to fill e-mail address and phone number of each added case handler. Two factor authentication functionality, possible for each user to add. Logging of each action from each user. Time limitations for using the system and being inactive.	Who has been consulted? Data Protection specialists at law firm	Accepted	No

7.	Administrator or Case handler is part of the report	The whistleblower has the right and possibility to report any person in the company.	Risk that the reported person has access to the report as administrator or case handler, and potentially can destroy evidence and/or close the case without further investigation.	High	In our onboarding instructions, we recommend the client to always be more than one who have access to all whietleblower reports. Logging of all taken action in the system. It´s possible for the client to add Intake Management from a third party and request that the third party remove any details of the whistleblower, if the whistleblower anyway have left details in the report.	Data Protection specialists at law firm	Accepted	No

2. Instructions for completing the PIA-register

2.1 The processing

Here the processing is described. A reference can be made to the specific processing in the record of processing activities. Please note that the following must be described: the relevant personal data, the recipient of the personal data, the retention, a description of the processing including the nature, scope, context and purpose of the processing. Furthermore, the assets and/or the tools necessary for the personal data (hardware, software, network, persons, paper or paper distribution channels) must be specified. Adherence to approved codes of conduct should also be considered. If any of these factors are missing in the record of processing activities, they can be listed in the table above.

2.2 The necessity and proportionality of the processing

Indicate the factors that contribute to the processing being proportional and necessary in light of the legal basis (in case of legitimate interest being the legal basis, the specific interest shall be specified), the scope of the data processed and possible limited retention. Also indicate factors that strengthen the rights of the data subjects, such as information to the data subject, right of access, data portability, correction, deletion, limitation of processing and the right to object. Processor relationships and protective measures for international transfers shall also be included here. A reference can also be made here to the specific processing in the record of processing activities.

2.3 Risks

Describe the risks associated with the processing activities; sources of risk, threats that may lead to unauthorized access, unsolicited alteration or loss of data as well as potential impact on the risk of the rights and freedoms of the persons concerned. Rights and freedoms primary concern data protection and integrity, but may also include other fundamental rights, such as freedom of expression, freedom of thought, free movement, prohibition of discrimination, right to freedom, conscience and religion. Examples of risks may include the risk of unauthorized access to/or copying of personal data, accidental disclosure of personal data, intentional/accidental manipulation of data and risk of harmful code.

Indicate also if the risk is unlikely, potential, likely or highly probable.

2.4 Vulnerability

Estimate the level of vulnerability in relation to the identified risk based on three levels; low, middle, or high.

2.5 Measures

Specify what measures will be implemented to manage the risk/risks. For example, use of better passwords, improvement of the users’ knowledge of data protection, limitation of the number of authorized persons or improved technical security through new antivirus systems.

2.6 Participation of other parties

Indicate whether the data protection officer or other appropriate party has been consulted in connection with the implementation of the PIA. If appropriate, considerations from the data subjects or from their representatives should also be collected.

2.7 Risk after the measures

Indicate if the risk is eliminated, reduced or accepted.

2.8 Is a prior consultation with the supervisory authority necessary?

Indicate whether prior consultation with the supervisory authority is necessary. If the vulnerability of an identified risk is still considered to be high and the estimated probability of the risk being realized (despite the measures taken to reduce the risk) is not unlikely in accordance with the above PIA, a consultation shall be initiated with the competent supervisory authority prior to the initiation of the processing.

3. Measure overview

Indicate the measures to be taken according to the above PIA, the planned date of implementation and who is responsible for the implementation. If consultation with the supervisory authority is deemed necessary, such consultation shall be included as a measure in the table below.

No.	Measure	Date of implementation	Responsible person
1.	Develop functionality which makes it possible for the client to immediate delete the case without further storage, if irrelevant report which includes personal data.	March 2022	Product Manager
2.	Anonymize and pseudnymize functionality to be developed	December 2021	Product Manager