V17 Report DPIA Payroll Detect 2025 v1.0

Peple B.V.

Table of contents

1 Purpose of this DPIA

To assess and mitigate the risks to individuals' rights and freedoms related to the processing of their personal data. Specifically, it would focus on the potential impact of using AI to analyze sensitive payroll information

This DPIA aim to:

- **Identify and assess the risks:** This includes risks related to:
    - **Accuracy and bias:** Is the AI tool accurate? Could it produce false positives or negatives? Is there a risk of bias in the AI's algorithms that could unfairly impact certain groups of employees?
    - **Data security:** How is the data protected during transfer to the vendor, during processing, and at rest? What security measures does the vendor have in place? Are there robust data breach notification procedures?
    - **Transparency and explainability:** Can employees understand how the AI tool works and why it flagged a particular payslip as anomalous? Is there a risk of "black box" decision-making?
    - **Proportionality:** Is the use of AI for this purpose proportionate to the legitimate aim of identifying anomalies? Could less intrusive methods be used?
    - **Individual rights:** How will employees' rights be protected, such as their right to access, rectify, or erase their data? How will they be informed about the use of the AI tool? How can they object to the processing?
    - **Control:** Do employees have sufficient control over their data and the AI's processing of it?
- **Develop mitigation measures:** Based on the identified risks, the DPIA should outline specific measures to mitigate those risks. Examples include:
    - **Data anonymization or pseudonymization:** Where possible, use anonymized or pseudonymized data for training and testing the AI tool.
    - **Data minimization:** Only share the minimum necessary data with the vendor.
    - **Strong contractual safeguards:** Include robust data protection clauses in the contract with the vendor, ensuring compliance with GDPR and other relevant regulations.
    - **Human review:** Implement a process for human review of all AI-generated flags before any action is taken.
    - **Transparency and communication:** Clearly communicate to employees how their data is being used and what their rights are.
    - **Regular audits and monitoring:** Conduct regular audits of the AI tool and the vendor's data processing activities.
- **Document the DPIA process:** The DPIA itself should be thoroughly documented, including the assessment of risks, the mitigation measures, and the rationale behind the decisions. This documentation is crucial for demonstrating compliance with GDPR.

- **Consult with stakeholders:** Consult with relevant stakeholders, such as employees, works council, where necessary, during the DPIA process.

2 Scope and users

2.1 Scope

The scope of this document corresponds to that of the ISMS as defined in *B01 Information security policy Peple B.V.*.

2.2 Users

The users of this document are:

- De initiator of this DPIA
    - Makes decisions regarding the processing based on this DPIA.
- IT & Compliance Officer.
    - Coordinates the implementation of security measures and advice if the processing complies with the AVG legislation.

3 Related documents

This document is related to the following documents from the ISMS of Peple B.V.:

- Uses the scope as stated in **B01 Information security policy**.
- Is managed as stated in **B02 Document management**.
- It follows the principles outlined in **B17 Change management**.
- It adheres to the procedure outlined in **P17 Procedure DPIA.**

4 Description of Data Processing

4.1 Context

At Peple, we believe in smart technologies that make work easier and better. AI is a powerful tool for innovation, streamlining processes, and accelerating progress. That's why we continue to invest in AI and automation to make your HR and payroll administration more accurate, efficient, and future-proof. We work with Visma Resolve for this, a specialist in AI-driven work processes and part of the Visma Group.

Earlier, we informed you that Visma Resolve was introduced as an optional data processor. However, we have decided to include this functionality as standard in our product. This means you benefit from automated checks that detect errors faster, saving you time and reducing manual work.

In addition, Visma Resolve helps you with compliance and risk management, so you always comply with the latest laws and regulations. The AI tool detects deviations in salary processing, for example, in the event of collective bargaining agreement changes or tax rules, allowing you to take proactive action and prevent problems before they have an impact.

AI is not only a way to improve existing processes, but also a driving force behind innovation in HR and payroll software. It helps with error detection, but also provides valuable insights and predictions that support you in strategic decisions. By integrating AI as standard, we ensure that you are prepared for the future and continue to benefit from the latest developments. In addition, the AI models continuously improve themselves, making them increasingly smarter and more effective.

By making Visma Resolve available to everyone, we offer a consistent and high-quality service and help you to continue working optimally not only today, but also tomorrow.

4.2 Nature and Scope of Data Processing

The subprocessor's processing of personal data on behalf of the processor shall mainly pertain to: Storing, hosting, computing, modeling, data pre- and post-processing.

The duration of the processing of personal data is for as long as the Service Agreement applies.

4.3 Process steps, Categories of personal data/subjects, and Retention periods

- Pseudonymised employee IDs
- Optional pseudonymised employee groupings, i.e. contracts, departments or position types.
- For the payslips of the pseudonymised employee IDs:
  - Paycodes for the payslip transactions
  - Types of payslip transactions: e.g. salary, hours, tax deduction
  - Amount, rate, and quantity for the payslip transactions
  - Optional pseudonymised contract IDs for transactions

Process step	***Categories of personal data***	***Categories of individuals***	***Characteristics of Process Step (manual, automated, data exchange)***	***Retention Period***
Share data from Visma.net Payroll to Resolve	*-Pseudonymised employee IDs* *-Pseudonymised employee groupings, i.e. contracts, departments or position types.*	*Customer Employees*	*Automated*	*as long as the contract is active*
Receive results from Resolve back to Visma.net Payroll	*-Pseudonymised employee IDs* *-Pseudonymised employee groupings, i.e. contracts, departments or position types.*	*Customer Employees*	*Automated*	*as long as the contract is active*

4.4 Legal basis and purposes of processing

4.4.1 Article 6 and Article 9

Fill in for the 'ordinary' personal data. That means the personal data that:

1. Do not fall into the category mentioned in Article 9.
2. Are not BSN (Citizen Service Number).
3. Are not criminal data.

Article 6, section	Explanation of legal basis	Applicable yes/no, if *yes, specify the legal basis*	Purpose under this legal basis
Consent *(Article 6, Section 1, Subsection a)*	Processing personal data is lawful if the data subject has explicitly given consent for the processing of their data for a specific purpose.	No	
Performance of a contract *(Article 6, Section 1, Subsection b)*	Personal data may be processed if it is necessary for the performance of a contract to which the data subject is a party or to take pre-contractual measures at the request of the data subject.	Yes	*To deliver a more sufficient way of working.*
Legal obligation *(Article 6, Section 1, Subsection c)*	Processing is necessary for compliance with a legal obligation to which the controller is subject.	No	
Protection of vital interests *(Article 6, Section 1, Subsection d)*	If processing is necessary to protect the vital interests of the data subject or another natural person, this can serve as a legal basis.	No	
Performance of a task of public interest or exercise of public authority *(Article 6, Section 1, Subsection e)*	Processing is allowed if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority delegated to the data controller.	No	
Legitimate Interest *(Article 6, Section 1, Subsection f)*	If processing is necessary for the legitimate interests pursued by the data controller or a third party, and these interests do not override the interests or fundamental rights and freedoms of the data subject, this can serve as a legal basis. A balancing test must always be conducted to determine if the legitimate interest outweighs the privacy interests of the data subject.	No	

Fill this in for the special categories of personal data:

Lid, Article 9 GDPR	Explanation	Applicable yes/no, if yes, specify the legal basis	Purpose under this legal basis
Consent *(Article 9, section 2, subsection a)*	Processing of special categories of personal data is lawful if the data subject has explicitly given consent for the processing of this data for a specific purpose.	*No sensitive data is processed*	
Performance of legal obligations in the field of employment law, social security, and social protection systems *(Article 9, section 2, subsection b)*	Processing is allowed if necessary for the performance of legal obligations in the field of employment law, social security, and social protection systems, and only under specific conditions	*No sensitive data is processed*	

Protection of vital Interests *(Article 9, section 2, subsection c)*	If processing is necessary to protect the vital interests of the data subject or another natural person, this can serve as a legal basis.	*No sensitive data is processed*	
Processing by a foundation, association, or other non-profit legal entity *(Article 9, section 2, subsection d)*	Processing of special categories of personal data is permitted by foundations, associations, or other non-profit legal entities, provided certain conditions are met.	*No sensitive data is processed*	
Processing by political parties *(Article 9, section 2, subsection e)*	Processing of special categories of personal data is allowed by political parties under certain conditions.	*No sensitive data is processed*	
Processing by trade unions *(Article 9, Section 2, Subsection f)*	Processing of special categories of personal data is allowed by trade unions under certain conditions.	*No sensitive data is processed*	
Processing for reasons of public interest in the field of public health *(Article 9, Section 2, Subsection g)*	Processing of special categories of personal data is allowed for public health purposes, such as public health surveillance, medical diagnosis, healthcare management, and healthcare systems, under specific conditions.	*No sensitive data is processed*	
Processing for archiving purposes in the public interest, scientific or historical research, or statistical purposes *(Article 9, Section 2, Subsection j)*	Processing of special categories of personal data is allowed for archiving purposes in the public interest, scientific or historical research, or statistical purposes, under specific conditions.	*No sensitive data is processed*	

4.4.2 BSN

The BSN of the employee will not be shared because there is no need for it.

4.4.3 Criminal data

No data on criminal records will be shared for this functionality.

4.4.4 General Purposes of Processing

The purpose of the subprocessor's processing of personal data on behalf of the data processor is:

Delivering of services in accordance with the Service Agreement.

4.5 Involved parties

Name of involved party	***Role in the processing (controller,(sub) processor, joint controllers)***	***Location of this part of the data processing (EU/Non-EU)***	***If the processing does not occur***

			in the EU, explain.
Visma Resolve	processor	EU	-
Mixpanel, Inc.	sub processor	EU	-
Amazon Web services (AWS)	sub processor	EU	-
Visma E-conomic A/S	sub processor	EU	-
Visma Labs SIA	sub processor	EU	-
Visma Software International	sub processor	EU	-

An at all times up to date list of subprocessors is available from the Trust Centre.

4.6 Specific details

Supplier	***Functionality***
Visma Resolve	Visma Resolve is the developer of the AI tool that we use.
Mixpanel, Inc.	Mixpanel is a tool that is used to gain analytics.
Amazon Web services (AWS)	The software of Visma Resolve is hosted in AWS. Our visma.net Payroll product is also hosted in AWS so for that matter there is no different processor.
Visma	All other Visma subprocessors are used for billing and local support and do not process any of our customer data.

5 Proportionality and subsidiarity

In this chapter, we explain why the processing complies with the requirement of proportionality and subsidiarity (necessity and proportionality). Proportionality means that the intrusion into the personal sphere and the protection of the personal data of the data subjects are in proportion to the processing purposes. Subsidiarity means that the processing purposes are reasonably achieved without adversely affecting the data subjects in other, less disadvantageous ways.

5.1 Proportionality

Benefits and Necessity
Our service has been developed to save significant time and money for the users when utilized as intended. The primary benefits include:

-Efficiency: By automating routine tasks, the service allows users to focus on more strategic activities, increasing operational efficiency.
-Cost-Saving: The reduction in manual effort translates directly into cost savings, improving the economic feasibility for users.
-Scalability: Our system is designed to scale seamlessly with user needs, providing flexible solutions without the need for additional data collection.

Balancing Risks and Benefits

The proportionality of our service derives from its ability to balance minimal risks with substantial benefits. The design and implementation of the service ensure:

The processing of personal data is limited and justified in light of the significant advantages provided to the users.

Security measures in place are commensurate with the level of sensitivity of the data processed.

Our commitment to transparency ensures that users are informed about how their data is used, maintaining trust and confidence in the service.

Overall, our service exemplifies proportionality by aligning processing activities with user expectations and legal obligations, ensuring that data protection rights are respected while delivering substantial functional benefits.

5.2 Subsidiarity

The principle of subsidiarity is adhered to by ensuring that the processing purposes are effectively achieved in ways that are minimally detrimental to data subjects. Our approach involves implementing all feasible measures to mitigate potential risks while achieving processing objectives. This ensures that the rights and interests of data subjects are respected and protected throughout the data processing lifecycle.

6 Rights of data subjects

Article GDPR	How is compliance ensured for this processing
Right to information (Articles 13 and 14 GDPR)	We have a procedure for all requests from data subjects which can be filed here: https://www.visma.com/trust-centre/privacy-request
Right of access to personal data (Article 15 GDPR)	
Right to rectification of inaccurate data (Article 16 GDPR)	
Right to erasure ("right to be forgotten") (Article 17 GDPR)	
Right to restriction of processing (Article 18 GDPR)	
Right to data portability (Article 20 GDPR)	
Right to object to processing (Article 21 GDPR)	
Right not to be subject to automated decision-making (Article 22 GDPR)	
Right to withdraw consent (Article 7 GDPR)	
Right to lodge a complaint with a supervisory authority (Article 77 GDPR)	

7 Advice from the IT & Compliance Officer

Because we use pseudonymised employee ID's it is impossible for other processors to link payslips to a person. The AI tool only gives alarms and does not make any changes on its own. This mitigates almost every risk. Things we need to take into account are:

-**Data deletion;** We are responsible for deleting customer data when the contract is terminated. Make sure we have a clear procedure on when and how to delete customer data.

-**Configuration;** We need to make sure that we are not sharing more data than is strictly necessary. Builtin recurring checks to see if our API is configured correctly.

-Supplier assessment; Every year the asset owner needs to perform a supplier assessment (A12 Periodic supplier assessment (quality) v1.0) to check whether the supplier still meets our requirements and works to our expectations.

-**Customer satisfaction;** We need to make sure that this functionality delivers a great value to the customer so the sharing of data is for a good reason.

-Correct; We need to stay aware if the results are accurate. Make sure we keep receiving feedback from our customers on this topic and that we are able to make adjustments if we keep getting false positives.

8 Attachments

8.1 Risks and technical & organisational measures

Risk measures: We only share a minimum of data that is needed. There is no way to see which payslip belongs to which person.

We do a yearly supplier assessment to determine if the function is still adding value.

We ask for feedback from our customers to see if the detections that are provided are correct.

Technical measures: We build a secure API connection to make sure the data is fully encrypted when sharing it with Resolve.

Organisational measures: We have created a procedure for the on- & offboarding of customers to make sure we send the correct data and delete data the right way as soon as a customer ends the contract.

8.2 Authorisation Matrix for Access to Personal Data

No employees of the subprocesser have direct access to personal data.
The configuration is managed by Peple.

8.3 A diagram of the network and related physical, procedural measures

N/A

8.4 Procedural measures regarding employees and facility services.

Procedures on deleting customer data have been implemented but are not shared due to confidentiality.