DPIA -Odoo system

Step 1: Identify the need for a DPIA

The project involves the use of an Odoo staging environment to test and validate system updates, bug fixes, and customisations before they are deployed to the production environment. This includes functional testing, regression testing, and user acceptance testing (UAT) to ensure that all changes meet business requirements and do not introduce new issues.

A Data Protection Impact Assessment (DPIA) is required because the Odoo staging environment processes real personal data for this purpose.

In this case, data anonymisation or masking is not feasible due to the complexity of the workflows being tested and the need for realistic data to ensure accurate validation. As a result, identifiable information such as customer, employee, or transaction data may be temporarily processed in a non-production environment.

Given the potential risks to data subjects—such as unauthorised access, data leakage, or misuse—a DPIA is necessary to assess and mitigate these risks and to ensure compliance with data protection regulations

Step 2: Describe the processing

Data Collection

- Data is copied directly from the production environment at the point when testing is required.

Data Use

- Simulate real transactions and workflows
- Validate the accuracy and stability of new features or fixes
- Perform regression and user acceptance testing

Data Storage

- Data is temporarily stored in the staging database, which is isolated from production and accessible only to authorised personnel.
- Access is controlled via role-based permissions and audit logging.

Data Deletion

- Once testing is complete and changes are validated, the staging data is permanently deleted.
- The staging environment is not used to merge or sync data back into production

Data Source

- The sole source of data is the production Odoo environment

Data Sharing

- No data is shared externally.
- Access is limited to internal development and QA teams with a legitimate need to perform testing

The processing of personal data in the Odoo staging environment is strictly limited to testing purposes only. This includes validating system updates, bug fixes, and customisations prior to deployment in the production environment.

Nature of the Data

The data used for testing may include:

- Basic personal information (e.g., name, contact details)

- Transactional data (e.g., sales orders, invoices)
- Employment-related data (e.g., job roles, departments)
- Special category data, specifically non-medical health information (e.g., dietary needs or accessibility requirements)

No criminal offence data is processed.

Volume and Frequency

- Data is copied from the production environment only when testing is required.
- The volume reflects a snapshot of the production database at that time.
- Testing is conducted on an as-needed basis, not continuously.

Retention

- Data is retained only for the duration of the testing activity.
- Once testing is complete and validated, the data is securely deleted from the staging environment.
- No data is merged back into production.

Individuals Affected

- The number of individuals affected depends on the scope of the copied dataset, which may include customers, employees, or vendors.

Geographical Scope

- The data relates to individuals primarily located in the areas Microlink operates its business.
- The staging environment is hosted in a secure location compliant with applicable data residency requirements.

Nature of the Relationship with Individuals

The individuals whose data may be processed in the Odoo staging environment are primarily:

- **Customers**, who have interacted with the organisation through purchases or service requests
- **Vendors or partners**, involved in procurement or service delivery

These individuals have an established relationship with the organisation, typically through contractual or service-based interactions.

Control and Expectations

- Individuals do not have direct control over how their data is used in the staging environment.
- However, the use of their data for internal testing purposes is considered a legitimate interest of the organisation, provided appropriate safeguards are in place.
- While individuals may not explicitly expect their data to be used in a test environment, this is a common and necessary practice in system development and quality assurance, especially when anonymisation is not feasible.

Vulnerable Groups

- The dataset may include employees or customers with accessibility health-related needs, but it does not include children or other vulnerable groups.
- Any special category data (e.g., non-medical health information) is handled with heightened care and restricted access.

Prior Concerns or Security Flaws

- There have been no known prior incidents or security breaches related to the use of the staging environment.
- The environment is isolated from production and access is limited to authorised personnel only.

Novelty and Technology

- The use of a staging environment for testing ERP systems like Odoo is not novel and follows standard industry practices.
- The current state of technology supports secure, isolated environments for testing, and the organisation leverages these capabilities to minimise risk.

Public Concerns

- There is increasing public awareness and regulatory scrutiny around the use of real personal data in non-production environments.
- This DPIA reflects the organisation's commitment to transparency and responsible data handling in response to those concerns.

Codes of Conduct or Certification

- The organisation is **not currently signed up to an approved code of conduct or certification scheme** specific to data protection, as none have been formally approved under GDPR at this time.
- However, internal policies and procedures are aligned with recognised best practices and regulatory requirements.

The primary purpose of processing personal data in the Odoo staging environment is to test and validate system changes—including bug fixes, updates, and customisations—before they are deployed to the live production environment.

What We Want to Achieve

- Ensure that new features and fixes function correctly
- Identify and resolve issues before they impact end users
- Maintain the stability, accuracy, and performance of the Odoo system

Intended Effect on Individuals

- There is no direct impact on individuals, as the processing occurs in a non-production environment.
- Indirectly, individuals benefit from a more reliable, secure, and user-friendly system.
- The use of real data ensures that testing reflects actual use cases, reducing the risk of errors in live operations.

Benefits of the Processing

For the organisation:

- Reduces the risk of deploying faulty or insecure code

- Improves system quality and user satisfaction
- Supports compliance by ensuring updates do not compromise data integrity or security

More broadly:

- Promotes responsible software development practices
- Enhances trust in digital services by ensuring systems are thoroughly tested before release

Step 3: Consultation process

Consulting Individuals (Data Subjects)

Direct consultation with individuals whose data may be processed in the staging environment is not considered appropriate or necessary in this context. This is because:

- The processing is limited to internal testing purposes.
- There is no direct impact on individuals.
- The data is not used to make decisions about individuals or affect them in any way.
- Appropriate safeguards (e.g. access controls, data deletion after testing) are in place to minimise risk.

However, the organisation remains transparent about its data handling practices and is committed to upholding data subject rights.

Internal Stakeholders to Involve

- **Data Protection Officer (DPO)** or privacy lead: To review and approve the DPIA and ensure compliance with data protection laws.
- **IT and Development Teams**: To provide technical details about the staging environment, data handling, and security controls.

External Processors

If any third-party processors (e.g. hosting providers, consultants) are involved in managing the staging environment, they may be asked to:

- Confirm their compliance with data protection obligations.

- Provide documentation on their security measures.
- Support data deletion and access control procedures.

Expert Consultation

- **Information Security Experts**: Will be consulted to assess and validate the technical safeguards in place (e.g. access controls, encryption, network isolation).
- **Legal or Compliance Advisors**: May be consulted if there is uncertainty about the lawful basis or risk level of the processing.

Step 4: Assess necessity and proportionality

The lawful basis for processing personal data in the staging environment is legitimate interest under Article 6(1)(f) of the GDPR. The organisation has a legitimate interest in ensuring the reliability, security, and functionality of its systems through thorough testing before deployment.

Purpose Achievement

The processing is necessary to:

- Validate system changes in realistic conditions
- Prevent errors or data loss in production
- Ensure compliance with business and regulatory requirements

This processing directly supports the intended purpose and cannot be effectively achieved using anonymised or synthetic data due to the complexity of the workflows being tested.

Alternatives Considered

- **Anonymisation or masking** was considered but deemed not feasible due to the need for realistic data to test complex, interdependent modules and workflows.
- No other method provides the same level of assurance in testing accuracy and system integrity.

Preventing Function Creep

- The staging environment is used exclusively for testing and is not repurposed for analytics, training, or other secondary uses.
- Access is restricted to authorised personnel, and data is deleted after testing is complete.

Data Quality and Minimisation

- Data is used in its original form to preserve integrity during testing.
- While data minimisation is not feasible in this context due to the need for complete and relational datasets, the organisation ensures that:
  - Data is only copied when testing is required
  - The staging environment is isolated and access-controlled
  - Data is deleted immediately after testing is completed

Transparency and Information to Individuals

- While individuals are not directly notified about each test cycle, the organisation's privacy notice should include information about internal testing and quality assurance practices.
- The organisation is committed to transparency and will update its privacy documentation as needed.

Supporting Data Subject Rights

- Although the staging environment is not accessible to data subjects, their rights (e.g., access, rectification, erasure) are respected in the production environment.
- Any data copied for testing is temporary and not used to make decisions about individuals.

Processor Compliance

- If any third-party processors are involved (e.g., hosting or support services), they are bound by data processing agreements (DPAs).
- Processors are required to implement appropriate technical and organisational measures and are subject to regular review.

Safeguarding International Transfers

- The staging environment is hosted within the organisation's designated region UK to ensure compliance with data residency requirements.
- If any international transfers occur, they are governed by Standard Contractual Clauses (SCCs) or other approved transfer mechanisms under GDPR.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm (Remote, possible or probable)	Severity of harm (Minimal, significant or severe)	Overall risk (Overall risk - High, Medium, Low)
Use of real personal data in a non-production environment may lead to unauthorised access or accidental exposure. This could result in privacy breaches, reputational damage, and regulatory penalties.	Remote	Significant	Low
Inability to fully anonymise or minimise data due to complex database structures increases the risk of overexposure of sensitive information.	Remote	Significant	Low
Access by unauthorised internal users due to misconfigured permissions or lack of access controls could lead to data misuse.	Remote	Significant	Low
Failure to delete test data after use could result in unnecessary retention of personal data, violating data minimisation and storage limitation principles.	Possible	Minimal	Low
Processing of special category data (e.g., non-medical health information) without adequate safeguards could lead to discrimination or harm to individuals.	Remote	Significant	Low
Lack of transparency to data subjects about	Possible	Minimal	Low

the use of their data in testing may raise trust and compliance concerns.			

Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in the above				
Risk	**Options to reduce or eliminate risk**	**Effect on risk (Eliminated reduced accepted)**	**Residual risk (Low medium high)**	**Measure approved (Measure approved)**

This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA