EN

CERRIX

Data Protection Impact Assessment (DPIA)

CERRIX B.V.

CERRIX

Document management

Information about this document and version are shown in the tables below.

Document Properties

Classification:	CERRIX Public
Subject:	Data Protection Impact Assessment
Author(s):	R.M. van der Horst, J Jonkers
Initial date of effect:	
Current version:	1.2
Status:	Done
Distribution:	CERRIX stakeholders

Version Management

Version	Date	Author	Description of changes
1.0	10-01-2024	R.M. van der Horst	Initial version
1.1	03-04-2025	R.M. van der Horst	Annual review of the DPIA. No changes necessary.
1.2	06-08-2025	J Jonkers	Fixed typo's and classification

CERRIX

Table of Contents

1. Introduction

A Data Protection Impact Assessment (DPIA) is a process required by the General Data Protection Regulation (GDPR) to assess the potential impact of data processing activities on the privacy and protection of individuals' personal data. It is used to identify and mitigate risks that could arise from the processing of personal data, particularly when those activities are likely to pose a high risk to the rights and freedoms of individuals.

1.1 Purpose

To systematically evaluate how personal data is processed, identify privacy risks, and ensure that appropriate measures are in place to mitigate those risks.

1.2 Scope

The Scope of this DPIA is limited to the CERRIX GRC platforms we deliver and maintain as a SaaS product.

1.3 Intended audience

Customers of the CERRIX GRC platform whose data is impacted.

CERRIX

2. Data Protection Impact Assessment

Risk	Impact	Likelihood	Mitigation	Residual Risk
Unauthorized access to customer data	High	Medium	▪ Strong Password requirements ▪ Multi-Factor Authentication ▪ Role Bases Access Control	Low
Data breach due to insufficient encryption	High	Low	▪ Encryption-at-Rest ▪ Encryption-in-Transit ▪ Encrypted Backups	Low
Data loss due to software bugs	High	Medium	▪ Regular updates ▪ Automated backups	Low
Unauthorized processing of customer data by employees	High	Low	▪ Automated Backups ▪ Employee screening ▪ Logging & Audit trails ▪ Privileged Identity Management	Low
Data loss due to inadequate backup policy	High	Low	▪ Automated backups ▪ Periodic testing of backup ▪ Periodic Restore testing	Low
Excessive retention of customer data	Medium	High	▪ The customer is the data controller and therefore responsible for data retention. CERRIX will help facilitate.	Low
Non-compliance with GDPR requirements for data processing	High	Medium	▪ Data Processing Agreements with Third-Parties ▪ Internal Audits ▪ External Audits	Low

Data breach due to exfiltration	High	Medium	▪ Security Operation Center ▪ Perimeter Security ▪ Defense-in-Depth	Low
Data breach by accidentally disclosing sensitive information due to human error.	High	Medium	▪ Awareness training ▪ Data classification & labelling ▪ Data loss prevention tools ▪ Encryption-in-transfer	Low

CERRIX

3. Record of Processing Activities

Processing Activity	Purpose	Data	Data Subjects	Legal Basis	Retention Period	Data Recipients
User account data	Login to CERRIX and use the platform	Name, Email	Employees	Necessary for use	Until customer admin deletes	Customer
Organizational Data	Meta data for structuring GRC	Organization name, Location(s), Departments	Customer	Necessary for use	Until customer offboarding	Customer
Risks	Risk register		Customer	Consent	Until customer deletes it	Customer
Controls	Control register		Customer	Consent	Until customer deletes it	Customer
Measures of Improvement	Mitigation measures		Customer	Consent	Until customer deletes it	Customer
Audit Data	Internal or External auditing	Audit findings	Customer	Consent	Until customer deletes it	Customer
Evidence	Control effectiveness		Customer		Until customer deletes it	Customer
Process	Registering processes and process risks	Flow charts	Customer	Consent	Until customer deletes it	Customer
Incidents	Incident register & reporting	Incident data	Customer	Consent	Until customer deletes it	Customer