EN

# Data Protection Impact Assessment (DPIA)

*This document is a DPIA for CERRIX's GRC SaaS solution.*

CONFIDENTIAL

CERRIX B.V.

# Document management

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

## Document Properties

| | |
|---|---|
| **Classification:** | CERRIX Confidential |
| **Subject:** | Data Protection Impact Assessment |
| **Author(s):** | R.M. van der Horst |
| **Initial date of effect:** | January, 2024 |
| **Current version:** | 1.1 |
| **Status:** | Final |
| **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** | 3-4-2025 | R.M. van der Horst | Annual review of the DPIA. No changes necessary. |

## CLASSIFICATION: CERRIX CONFIDENTIAL

This document has been classified as CERRIX Confidential. The information contained within this document and any accompanying appendices is exclusively meant for the addressees that this document is directly distributed to. Distribution of this document, its contents and attachments by any party or person other than those listed in the distribution list is prohibited unless explicit prior written permission is extended by CERRIX B.V. This document, its contents, and attachments are subject to a Non-Disclosure Agreement.

If you received this document in error and/or you do not have explicit permission in the sense stated above, CERRIX B.V. requests you close this document immediately and destroy it and any copies made.

Nothing in this document may be duplicated, in part or in its entirety, and/or made public by any means without prior written authorization of CERRIX B.V. No rights can be deduced from the content of this document.

# 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 who’s data is impacted.

## 2. Data Protection Impact Assessment

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

| | | | | |
|---|---|---|---|---|
| **Data breach due to exfiltration.** | High | Medium | ▪ Security Operation Center<br>▪ Perimeter Security<br>▪ Defense-in-Depth | Low |
| **Data breach by accidently disclosing sensitive information due to human error.** | High | Medium | ▪ Awareness training<br>▪ Data classification & Labelling<br>▪ Data Loss Prevention tools<br>▪ Encryption-in-transfer | Low |

# 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 |