



COMPLIANCE  
PARTNERS

# SECURITY WHITEPAPER

*Version 1.0,  
The 9th of January 2024*

*Kristoffer Pedersen*



Compliance Partners ApS  
Reg. No. 43615661  
Kultorget 11, 4., 1175  
Copenhagen C

# Table of Contents

<b>1</b>	Introduction	3
<b>2</b>	Human Resources	3
	<b>2.1</b> Background Checks	
	<b>2.2</b> Awareness & Training	
<b>3</b>	Identification & Access Management	4
<b>4</b>	Product Infrastructure	4
	<b>4.1</b> Physical & Environmental	
	<b>4.2</b> Network Security	
	<b>4.3</b> Encryption	
	<b>4.4</b> The Screening Team	
<b>5</b>	Direct Application	5
<b>6</b>	Incident Response	5
<b>7</b>	Privacy & Data	5



# 1. INTRODUCTION

Compliance Partners Group prioritizes your security and has published this Security Overview, to enhance transparency and accountability, which is part of our core values. This overview is intended to provide access to the mechanisms that protect your information when you are using our solutions.

Our information security controls and mechanisms are based on the ISO/IEC 27001 Standard, which is the world's best-known standard for information security management systems.

*“With cyber-crime on the rise and new threats constantly emerging, it can seem difficult or even impossible to manage cyber-risks. ISO/IEC 27001 helps organizations become risk-aware and proactively identify and address weaknesses” – ISO Standard Website.*

## 2. HUMAN RESOURCES

### 2.1 Background checks

Our employees undergo background checks during the employment process, which includes obtaining criminal records of Management, the Screening Team, and the Legal Team. All employees sign non-disclosure agreements (NDA) before gaining access to our systems.

### 2.2 Awareness and training

All employees will attend an information security training session during onboarding. The training gives the employee crucial knowledge on how to mitigate the threat of outsiders gaining access to information, how to handle confidential information, and the obligations in relation to whistleblowers and data protection regulation.



## **3. IDENTIFICATION & ACCESS MANAGEMENT**

To access our physical facilities employees, need to use a unique access code, and alarm systems are turned on after working hours. Furthermore, all employees are required to use a unique identification to access our systems. We enforce multi-factor authentication.

## **4. PRODUCT INFRASTRUCTURE**

### **4.1 Physical & Environmental**

Microsoft provides our cloud infrastructure. Microsoft implements and maintains appropriate technical and organizational measures to protect information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Those measures comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 2701.[1]

### **4.2 Network Security**

We have split our systems into separate networks so that we can retain user access and ensure that information access is limited to certain people.

### **4.3 Encryption**

Information that is in the process of being transferred over public networks to Microsoft, or between Microsoft data centers, is encrypted. All laptops are managed and encrypted by our Administration. The end users cannot disable antivirus software or any security features. Our IT team pushes updates periodically to ensure that all devices are running with the latest software version.

[1] [Microsoft Products & Services Data Protection Addendum.](#)



## 4.4 The Screening Team

Members of our Screening Team are selected with care and instructed in the Whistleblower Directive. It is ensured that the Screening Team is impartial in all cases.

## 5. Direct Application

We have established procedures for performing periodic scans of our systems. Results are evaluated in relation to importance and priorities and mitigated afterward.

## 6. Incident Response

We have created procedures for receiving security incident reports. Our incident response includes:

- Logging
- Categorization
- Investigation
- Containment
- Learning

## 7. Privacy & Data

Your personal data is kept confidential as well. You can read more about how we collect personal data in our Privacy Policy.

