



MASTER PEOPLE PLATFORM

WHITE PAPER: *SECURITY AND COMPLIANCE*

INTRODUCTION

Master People Platform is a suite of applications that allow business users to assess employees, project stakeholders and candidates. It is a platform for collecting data and perform analysis.

The platform is a cloud-based software solution (SaaS) consisting of two applications which can be accessed securely by users from a modern browser, and an API for system-to-system integrations.

LOCAL REQUIREMENTS

Master People Platform is accessible via a browser and do not require any special local infrastructure, except for a modern browser.

We strive to be usable from all modern browsers, but officially support the recent versions of the most common browsers on the marked.

These browsers are available on most platforms like Windows, MacOS, Linux, iOS, and Android on devices like Desktops, Tablets, and Phones.

We currently support:

- Chrome
- Edge
- Firefox
- Safari

COMMUNICATION AND PORTS

All access to Applications and API use HTTPS for communication. To ensure, that all services are accessible, please allow access to all our secure endpoints using port 443, TLS1.3.

- <https://app.master-hr.com>
- <https://api.master-hr.com>
- <https://metisweb.master-online.com>

Emails will be sent from:

- noreply@master-online.com



MASTER PEOPLE PLATFORM
For simple, faster & better HR decisions.

Strengthen recruitment and talent development with an easy-to-use assessment platform that makes accurate HR analytics come alive across all devices.



MASTER PEOPLE PLATFORM

WHITE PAPER: SECURITY AND COMPLIANCE

LOGIN

Users can login to Master People Platform using an email address as their personal identification. We support both using locally managed passwords combined with a one-time code for 2-factor authentication on login as well as integration to external trusted Identity Providers.

- Master Password + 2FA code
- Microsoft (Azure AD, Microsoft365 & Office)
- Google



Optionally, it is possible to implement custom SSO based on our support for OpenID and OAuth 2.0.

2FA – ALL LOGINS

The Master People Platform uses an e-mail PIN code to verify the user has legitimate access to the e-mail address used to login to the platform. Most users will be asked to confirm their access once or twice a day, but some will be asked to confirm more often depending on their Network settings (roaming between networks can trigger an authorisation request). This requirement is active on all login types (Master Password and External Services), users that login via the Master Password method will always be asked for a PIN on each login, but this section covers the scenario where Microsoft or Google logins are used, or users that leave the Portal open for extended periods of time.

We log multiple factors of network and browser information from each user on the system for the purposes of detecting changes of access which are then used to trigger a new PIN authentication process.

NOTIFICATIONS

Users and Test Takers are notified using an email service. Emails are sent using a cloud-based mailing service with whitelisting and reputation keeping as a part of the service.

The sender emails are:

- noreply@master-online.com
- noreply@master-hr.com

All email addresses and domains associated are DMARC compliant with DKIM and SPF alignment.

MASTER PEOPLE PLATFORM
For simple, faster & better HR decisions.

Strengthen recruitment and talent development with an easy-to-use assessment platform that makes accurate HR analytics come alive across all devices.



MASTER PEOPLE PLATFORM

WHITE PAPER: SECURITY AND COMPLIANCE

AUDIT

All user actions like login and access to data are audited in Master People Platform.

Events include date and time of the action, as well as the type of activity and relevant references to the affected data context.

Events related to activities relevant for invoicing are made available in summarized form to enable invoicing based on usage.

DATA SECURITY MEASUREMENTS

Data stored on the platform are protected by "Privacy by Design". The architecture implements a structure where personal data are stored separately from assessment results. By separating personal data and assessments results on two different database systems with separate authentication systems, we have made it impossible to relate data without access to both systems.

Collected assessment data are pseudonymised on the assessment store using a key. This key is stored with the person data on the personal data store. To relate assessment results to a specific person, you need authenticated access to both data stores.

This structure enforces automatic anonymization of assessment data when person data are deleted from the system along with the pseudonymisation key. The relation between person data and assessment cannot be recreated once the key is deleted.

ENCRYPTION AND DATA

Data handled by the platform are encrypted on three levels:

- Database and Storage
- Data Transport and Communication
- Application and Code

MASTER PEOPLE PLATFORM
For simple, faster & better HR decisions.

Strengthen recruitment and talent development with an easy-to-use assessment platform that makes accurate HR analytics come alive across all devices.



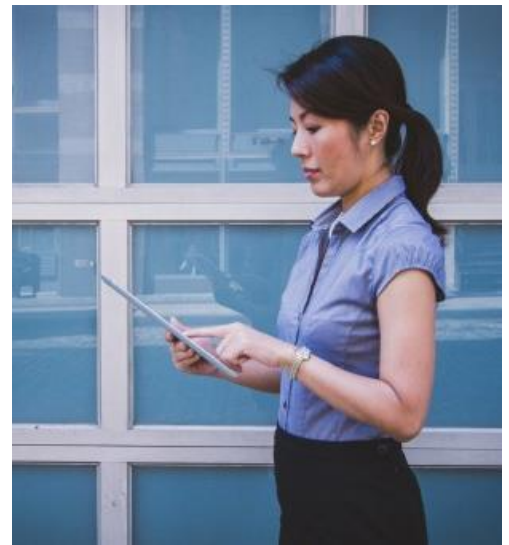
MASTER PEOPLE PLATFORM

WHITE PAPER: SECURITY AND COMPLIANCE

The platform utilized multiple storage and database technologies. All of them implements encryption on a service level. This means, that all databases perform real-time encryption and decryption of data, backups and transaction logs using the AES256 standard. Encryptions keys are managed and rotated in compliance with the internal security policy and the root key is protected by an internal secret store.

All communication between our services and clients are secured by a 2048-bit encryption certificate issued to Master International A/S by a trusted certificate authority. The encryption is implemented on all our services and supports HTTPS/TLS1.2+1.3 on all domains and endpoints used by the platform.

To ensure the integrity of our application, we use code-signing certificate issued by GlobalSign for all distributed applications. This digital signature preserves the integrity of the application and ensure that the application code is not altered with unapproved changes after release.



COMPLIANCE

Security and Compliance is important to us to ensure optimal data protection and governance. We are being audited and perform ongoing audit and risk assessment of our sub-suppliers.

MASTER PEOPLE PLATFORM

For simple, faster & better HR decisions.

Strengthen recruitment and talent development with an easy-to-use assessment platform that makes accurate HR analytics come alive across all devices.



MASTER PEOPLE PLATFORM

WHITE PAPER: SECURITY AND COMPLIANCE

Master International A/S

- ISAE 3000 Type II

Azure Hosting

- CSA STAR
- ISO 20000-1, 22301, 27001, 27017, 27018, 27701, 9001
- ENISA IAF
- EU Cloud CoC, EU GDPR, EU EN 301 549
- Germany C5 und IT-Grundschutz workbook
- Other: <https://docs.microsoft.com/en-us/azure/compliance/>

MASTER PEOPLE PLATFORM

For simple, faster & better HR decisions.

Strengthen recruitment and talent development with an easy-to-use assessment platform that makes accurate HR analytics come alive across all devices.