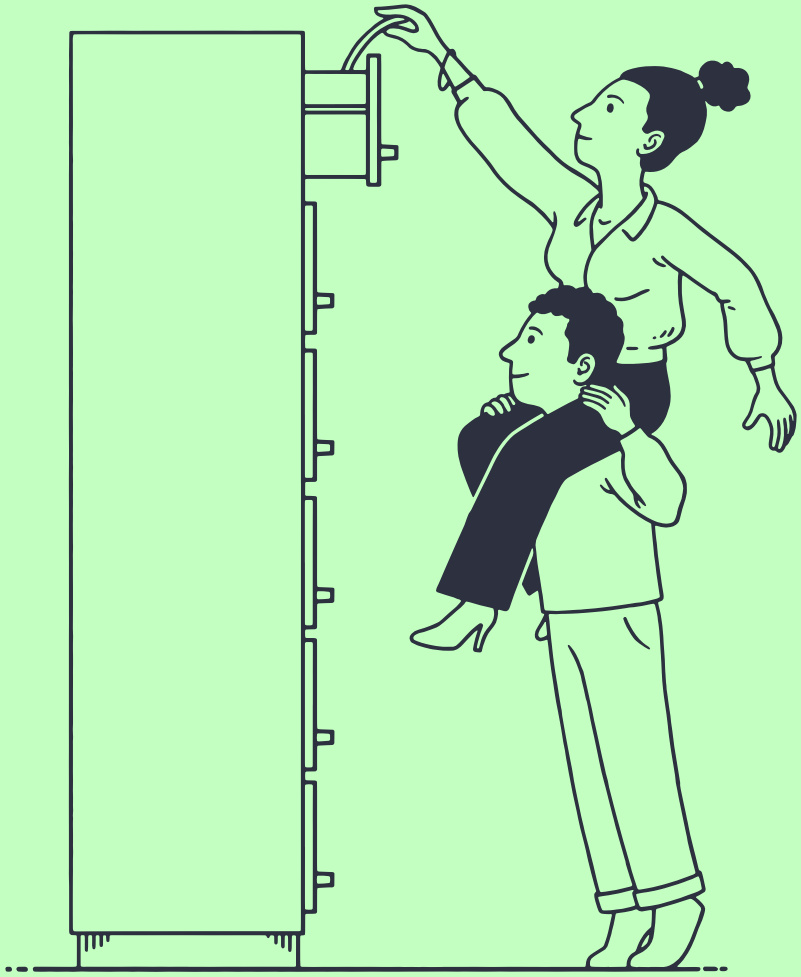
TECHNICAL SPECIFICATIONS

Data Security

We protect what matters most so you can focus on driving success.



HR:Duo
Automate. Comply. Thrive

hrduo.com

Data Security at HR Duo

Key Features

Advanced Encryption
Uses firewalls, HTTPS, and bank-level encryption to secure data and communications.

Secure Authentication
Authenticates over SSL/TLS and stores data in an encrypted form.

Segregated Data Protection
Segregates and tokenizes sensitive data for added security.

Access Control Measures
Restricts data access with two-factor authentication and strict permissions.

Continuous Security Monitoring
Performs regular scans, audits, and updates to maintain security.

CONTACT
datasecurity@hrduo.com
+44 121 295 7330

At HR Duo, we take your data as seriously as you do. It's one of your organisation's biggest priorities, so it's one of our greatest responsibilities.

We combine industry-standard best practice measures with our technology expertise, all wrapped around our understanding of your specific business and culture. This ensures the highest level of security, so you can focus your efforts instead on the people management and business initiatives that drive value. That's an HR headache taken care of.

How We Look After Your Data

Storage, Security and Privacy

- Employing firewalls, HTTPS, and bank-level encryption to secure networks, communications, and data for a higher level of security and privacy
- Authenticating over SSL/TLS (Transport Layer Security) and tokenizing and storing data in an encrypted data store
- Segregating and tokenizing all sensitive data, adding an extra layer of data protection

Secure Access Controls

- Storing data in a private cluster that's only accessible via two-factor authentication, for added physical and technical protection
- Maintaining a permissions-led regime that grants access only to those employees who need to see customer data for valid reasons

Data Kept Up-to-date

- Staying up-to-the-minute on security updates to software libraries, and applying any patches or bug fixes as needed to protect from threats
- Performing daily vulnerability scanning and assessment, as well as quarterly audits and risk assessments on services and data stores, to ensure we're adhering to our internal security policy requirements
- Maintaining internal security policies including network security, logical access, credentialing, passwords, and data classification
- Working with consultants and outside counsel to ensure our processes and controls are consistent with best practices

A Contracted Commitment

- Representing in our customer documentation that we will maintain a security programme consistent with industry standards
- Ensuring all clients are protected by a Data Processing Agreement