🔒 Data Storage & Privacy Policy

Last Updated: October 25, 2025
Effective Date: October 25, 2025

About

Version: 1.0.0
Created October 25, 2025
Updated October 25, 2025

License & Copyright

📋 Quick Summary

Demands Analysis is a web-based application for creating comprehensive job analysis documents. This application uses **localStorage** (browser local storage) to save your job analysis progress locally on your device. All data is **encrypted with your personal passphrase** before being stored using AES-GCM 256-bit encryption.

Key Points:

- ✅ **100% Client-Side**: All encryption happens in your browser
- ✅ **You Control Everything**: You choose when to save, load, or delete
- ✅ **Encryption**: AES-GCM 256-bit encryption with PBKDF2 key derivation
- ✅ **No Server Storage**: Your data never leaves your device
- ✅ **No Size Limits**: localStorage can handle large, complex forms (5-10 MB typical limit)
- ⚠️ **Your Responsibility**: If you forget your passphrase, your data is unrecoverable

🗄️ What Is localStorage?

localStorage is a browser feature that allows websites to store data on your device (computer, tablet, or mobile phone). Unlike cookies:

- **Larger Capacity**: 5-10 MB (vs 4 KB for cookies)
- **Persistent**: Data remains until explicitly deleted
- **Client-Side Only**: Never sent to servers automatically
- **Per-Origin**: Each website has its own isolated storage

In our application, localStorage serves **one primary purpose**: to allow you to safely close your browser without losing your progress on job analysis documents, including job descriptions, demands assessments, and work schedule information.

🎯 How We Use localStorage

Our localStorage usage is 100% user-controlled and privacy-focused:

1. **Opt-In Only**: We never store data without your explicit action
2. **Encrypted Always**: All data is encrypted before storage
3. **User-Controlled**: You decide when to save, load, or delete
4. **No Tracking**: We don't track your usage or behavior
5. **No Third-Party Sharing**: Your data stays on your device

What Gets Stored

When you click "Save Data for Later":

- **Job Information**: Job title, company name, job overview, and job functions (encrypted)
- **Demands Data**: Physical demands, mobility demands, cognitive/sensory demands, environmental demands, and lifting/pushing/pulling assessments (encrypted)
- **Work Schedule**: Hours per week, shift length, and shifts per week (encrypted)
- **Demographics**: Employee information and company details (encrypted)
- **Document Settings**: Brand colors, author information, and document title (encrypted)
- **All other form inputs**: Any additional data you've entered (encrypted)

What Does NOT Get Stored

- Your passphrase (never stored anywhere)
- Browsing history
- Personal identifiers
- Analytics data

🔐 Security & Encryption

Encryption Technology

We use **Web Crypto API** with industry-standard encryption:

Feature	Technology	Details
Encryption Algorithm	AES-GCM	256-bit Advanced Encryption Standard
Key Derivation	PBKDF2	100,000 iterations with SHA-256
Initialization Vector	Random	12 bytes, unique per encryption
Salt	Random	16 bytes, unique per encryption
Authentication	GCM Mode	Built-in authentication tag

How It Works

1. **You enter a passphrase** (e.g., "MySecretPhrase123")
2. **Key derivation**: Your passphrase is converted to a cryptographic key using PBKDF2 with 100,000 iterations
3. **Random salt & IV**: Unique random values are generated for this encryption
4. **Encryption**: Your form data is encrypted using AES-GCM 256-bit
5. **Storage**: The encrypted data (+ salt + IV) is stored in localStorage
6. **Decryption**: Only someone with your exact passphrase can decrypt the data

⚠️ User Risks & Responsibilities

What You Need to Know

This is a convenience feature, not a security vault. By using this feature, you acknowledge:

1. **Device Security**

- Anyone with access to your device can potentially access your data
- If your device is compromised (malware, keylogger), your data may be at risk
- Physical access to your unlocked device = access to your data

2. **Passphrase Security**

- **If you forget your passphrase, your data is PERMANENTLY LOST**
- There is no "password recovery" or "reset password" option
- We cannot help you recover your data if you forget your passphrase
- Choose a passphrase you will remember

3. **Browser Storage**

- Clearing browser data will delete your saved information
- Uninstalling your browser will delete your saved information
- Browser updates or crashes may corrupt localStorage data

4. **No Backup**

- Data is only stored on this device
- If you lose your device, you lose your data
- We do not have copies of your data

Legal Disclaimer

BY USING THIS FEATURE, YOU AGREE THAT:

- You use this feature at your own risk
- We are not liable for any data loss, theft, or compromise
- You will not hold us responsible for security breaches on your device
- You understand the technical limitations and accept them

🎛️ Managing Your Data

How to Control Your Data

Option 1: Use Our Built-In Controls

- **Save Data**: Click "Save for Later" button (stores encrypted data in localStorage)
- **Load Data**: Click "Load Saved Data" and enter your passphrase
- **Clear Data**: Click "Clear Saved Data" (removes all stored data)

Option 2: Browser Settings

You can also manage localStorage through your browser:

Chrome/Edge:

1. Press `F12` to open Developer Tools
2. Go to "Application" tab
3. Click "Local Storage" → your site URL
4. Right-click → "Clear"

Firefox:

1. Press `F12` to open Developer Tools
2. Go to "Storage" tab
3. Click "Local Storage" → your site URL
4. Right-click → "Delete All"

Safari:

1. Preferences → Privacy → Manage Website Data
2. Find your site → Remove

Data Expiration

- Saved data is marked to expire after **30 days**
- The application will show you how many days remain
- Expired data is automatically cleared on next visit

📊 Detailed Storage Information

Our localStorage Items

Item Name	Purpose	Encrypted	Size
`userFormData`	Your encrypted form data	✅ Yes	Variable (typically 10-500 KB)
`hasStoredData`	Flag indicating data exists	❌ No	~10 bytes
`dataExpiration`	Timestamp for expiration	❌ No	~20 bytes

Third-Party Cookies (QuillJS CDN)

The QuillJS rich text editor library (loaded from CDN) may set analytics cookies:

Cookie Name	Provider	Purpose	Duration
`_ga`	Google Analytics	Track QuillJS library usage	~2 years
`_ga_*`	Google Analytics	Enhanced analytics	~2 years

Note: These cookies track library usage statistics, **NOT your personal form data**. Your encrypted form data is completely separate and inaccessible to these analytics.

📜 Version History

- **v1.0.0** (October 25, 2025): Initial implementation

Remember: This is a convenience feature for saving your work. For highly sensitive data, consider using dedicated password managers or secure document storage solutions.