SECURITY

# Security & Privacy FAQ

### ▶ IS MY DATA PHYSICALLY STORED AT YOUR SITE?

All data and processing occur on the cloud using Amazon Web Services (AWS), which adheres to the strictest security standards in the world, incl. ISO, SOC, FedRAMP and HIPAA. This includes guarantees on physical securing, monitoring and logging across all hardware and services. More information on AWS security can be found at: AWS Cloud Security Compliance Hub.

### ▶ WHERE IS MY DATA HOSTED?

Your data is by default encrypted and stored in the EU, for both primary and back-ups hosting (hot-site). For our enterprise customers, we offer the ability to store data in the UK or USA.

### ▶ HOW DO YOU PROTECT MY DATA?

Your data is encrypted at the highest standard both at rest and in transit. Data at rest is encrypted using hardware security modules and key management services, whilst data in transit is secured using end-to-end HTTPS SSL/TLS encryption. We also offer daily backups at a different region to decouple localisation aspects, satisfying the strictest governance requirements.

### ▶ HAS SECURITY BEEN VERIFIED BY A CERTIFIED INDEPENDENT ASSESSOR?

Yes, we maintain certificates of penetration testing, performed by BCS/CREST certified, independent assessors. We will happily share these certificates as we go through infosec with you, along with other certifications like UK Gov’s Cyber Security Essentials and ISO 27001:2022.

### ▶ DO YOU SHARE MY DATA WITH OTHER VENDORS LIKE OPENAI?

No, we do not share any customer data with any 3rd party vendors, including LLM vendors like OpenAI. Our own LLM is private and fine-tuned to understand specialised project management lingo.

### ▶ HOW DO YOU SECURE ACCESS MY DEDICATED PLATFORM ENVIRONMENT?

We leverage a range of best-in-class security tools to protect your service against malicious actions and web exploits, incl. AWS Web Application Firewall, Amazon GuardDuty and AWS Shield Standard. We also use Amazon Detective to automatically investigate, analyse and quickly identify the root cause of potential security issues. In addition, our source code is hosted in private code repositories, where access is internally restricted to appropriately trained personnel, and protected using strong password policies, SSO and MFA authentication.

### ▶ CAN OTHER NODES & LINKS CLIENTS SEE MY DATA, OR BENEFIT FROM IT?

You own your data. No other customer can see your data, nor can they benefit from your data. Our infrastructure is architected in a way that enforces this distinction at a code level, guaranteeing data sovereignty and security (i.e., multi-tenancy pool architecture). This architecture is supported by dedicated user credentials which are linked to the tenant. In this way, each user is assigned to their respective tenant. In addition, your company's admin will have enterprise-grade role access controls to ensure that every company user sees project data that you want them to see.

Our AI is built in a similar spirit - learning from past performance happens solely from your own project's actualised data, and no learning is shared across different customers. This means that effectively, every project created in Nodes & Links has its own, tailored prediction model, taking into account all the nuances that make your project unique. You can find more details here

### ▶ CAN I SECURELY INVITE MY TEAM TO THE PLATFORM? HOW DO I CONTROL WHAT THEY SEE?

We offer advanced user permissions right out of the box, which your admin can use to securely define the actions that each user can do, along with the actual project data they can see. This is readily accessible via the platform's interface.

### ▶ DOES NODES & LINKS HAVE ACCESS TO MY DEDICATED PLATFORM ENVIRONMENT?

We do not have access to your dedicated platform environment. Unless you of course wish to invite someone from the Nodes & Links support team to help you out with something (and then you can safely and easily remove them).

### ▶ HOW DO YOU MAKE SURE THAT NODES & LINKS CONTINUES TO BE SECURE AGAINST EMERGING THREADS?

We use best practice techniques to ensure emerging threads are immediately assessed and addressed. We have internal policies for best practice SDLC, and deploy automated tools and services to identify emerging threats. We also perform automated vulnerability scans at the application layer on a daily basis to guarantee peace of mind.

### ▶ DO YOU PROCESS PERSONAL DATA?

No personal data is processed or transferred by the use of the service (as defined in GDPR and in accordance with EU guidelines - see Data Protection and Data controller and Processor).

### ▶ WE ARE BREAKING UP. WHAT HAPPENS TO MY DATA?

Once an account is closed, we immediately and securely dispose of your data. Your data has unique keys that link them to your own dedicated tenant in our system. Upon closing the account, the tenant is also closed, which triggers the disposal of all the data associated with it. We use best practice protocols like SDLC to automatically dispose of the data.