SECURITY

Security FAQ

Where does my data go? Where is it stored? Where is it processed?
Can you guarantee that my data will not leave the country?

IS MY DATA PHYSICALLY STORED AT YOUR SITE?

Our platform is a native cloud application - we do not store or process your data on our premise. All data and processing taking place on the cloud, using Amazon Web Services (AWS). AWS adheres to the strictest security standards as it stores and processes some of the world's most sensitive data. AWS guarantees security across various aspects of the physical location of their servers incl. limited physical access, monitoring & logging of all access, and Surveillance & Detection. You can find out more **here.**

IN WHAT COUNTRY DOES MY DATA RESIDE?

Your data, and associated disaster recover backups, is stored and processed in the EU (Dublin, Ireland), adhering to the strictest GDPR standards. We also give you the option to use UK as a location.

HOW IS MY DATA PROTECTED?

Once you log in to the platform and upload your data, we use HTTPS SSL/TLS encryption to securely transfer the data and trigger cloud-based processing units to do the number crunching. Whilst number crunching is taking place, sometimes data also needs to pass across various sub services within AWS (say from some storage unit to a CPU unit and then back). In these cases, intra-service communication is further protected by AWS standards of best practice.

CAN OTHER NODES & LINKS CLIENTS SEE (OR USE) MY DATA?

Your data can only be viewed and accessed by the users you invite to your own dedicated environment. No other Nodes & Links client can see or leverage the raw data you upload, like your .xer files. Behind the scenes, each Nodes & Links client has their own dedicated tenant, facilitated by our multi-tenancy architecture (more info here). 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, and can only see and leverage that data only. We also enforce best practice access policies to ensure that the user's identity (and therefore tenant subscription) cannot be compromised.

WE ARE BREAKING UP. WHAT HAPPENS TO MY DATA?

Once an account is closed, we immediately and securely dispose 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 the data.

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 IS MY DATA PROTECTED?

We record all actions made by any user to ensure we can satisfy any audit requests on your behalf, including log ins, user invitations and data uploads. We store this data in a protected database using Amazon Cognito Userpool (see more **here**).

CAN I SECURELY INVITE MY TEAM TO THE PLATFORM? WHAT IF I WANT TO CONTROL PERMISSIONS TO SOME OF THEM?

We offer advanced user permissions right out of the box, so you can securely share access with everyone in your team. We operate on a principle of least privilege, which means that you can only invite users to the level of your own permission, and lower (not higher). Every user that you invite on the platform first gets registered on your dedicated user directory. You can easily access and view this directory at any time, and if you are an admin you can also control the permissions of each user that is in that directory. Once a user is part of your platform directory, you can then invite them in any of the projects you upload to your dedicated environment. On invitation, you can choose between 4 roles that control the actions that the newly invited user can do, including limiting the ability to upload new data. You can easily create teams to help to manage large pools of users in an easy way.

HOW DO YOU SECURE AGAINST UNAUTHORISED ACCESS TO MY DEDICATED ENVIRONMENT AND NODES & LINKS SOURCE CODE?

We deploy best in class services to protect the identify of all Nodes & Links' users directory, incl. Amazon Cognito and User Pools (see more **here**). In a nutshell, a user can only access your environment if they have been invited by another user that is already on your environment. We also deploy a range of best in class services to protect against web exploits that may impact availability and security, incl. AWS WAF, 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 and MFA authentication.

NEW THREADS AND VULNERABILITIES ARE DISCOVERED ALL THE TIME. HOW DO YOU KNOW WHETHER ANY OF THOSE INFLUENCE THE NODES & LINKS PLATFORM?

We use best practice techniques to ensure any emerging threads are timely assessed and addressed. We use best in class tools and service to automatically identify and report relevant vulnerabilities. If one is identified, developments tasks are triggered to address them ASAP. Application layer vulnerability scans are also performed and reported automatically on a daily basis.