**SECURITY AT TALENTLI**

Effective from July 15, 2021

At Talentli we are committed to offering world class data protection standards to ensure your data is safe and your compliance requirements are met. Here you’ll find more information on how we approach security, and if you have additional questions feel free to get in touch at team@tlnt.li

**GDPR Commitment**

Talentli is commited to compliance with the General Data Protection Regulation, and meeting our legal obligation by helping our customers become compliant.

**Payment Information**

Talentli does not store any payment information.

**Company Personal Data**

Talentli will comply with all applicable Data Protection Laws in the processing of Company Personal Data and not process Company Personal Data other than on the relevant company’s documented instructions.

**Data Centre Security**

Our hosting environment is fully-redundant with disaster recovery procedures. Our cloud hosting provider maintain multiple certifications for its data centers, including ISO 27001 compliance, PCI certification, and SOC. In addition all data is encrypted both in transit and at rest using strong encryption. For more information about certification and compliance, please visit the … security site.

**Multi-Layer Encryption**

In addition to the industry standard in transit and at rest encryption of the data, we also utilise at-work encryption in our database, which ensures that sensitive bits of data are encrypted while database is working. This allows us to introspect, service, and operate our Services without having programmers and administrators inadvertently exposed to private data during the course of their work.

**Automated Tests**

We run an extensive suite of automated tests after each code change to verify correctness of Talentli features, including authentication and the permission system.

**Communication**

All user data is transported securely, as all traffic is encrypted in transit via SSL. Encrypting data in transit protects it from unauthorised snooping, modification, and man-in-the-middle attacks. We use 256-bit SSL/TLS.1.2 encryption, utilising both the ECDSA and RSA algorithms.

**Data Backups**

We run automated backups of our databases every day to ensure your data stays safe and highly available.

**HTTPS**

Our application forces all requests over HTTPS, ensuring all traffic is secured in transit and protecting against protocol downgrade attacks.

**Log Collection**

We collect detailed logs to ensure we have a high-resolution trail of the actions performed across the platform for any incident investigation if required.

**Security Headers**

Our application uses a series of security headers, including X-Frame-Options, X-XSS-Protection, and Content-Security-Policy to mitigate a wide range of common security issues.

**Software Updates**

We have automated systems in place that monitor the versions and vulnerabilities in all of the code that powers the Talentli system and our infrastructure is continously updated to the latest and most secure versions of software.

**Limited and Audited Employee Access**

Only the employees who need access to improve or operate the Talentli system have access. We make sure there are several layers of controls that individuals must go through to access customer data. And when they do their routine maintenance, debugging, or servicing of the Talentli system, they’re led through an auditing access path that requires them to state the valid consent or justification for the specific access session.

**Third Party Sub-Processors**

Our sub-processors are leaders in their space and have security as top priority. You can find the list of our sub-processors in our … page.

**Vulnerability Disclosure**

In the event of a data breach involving personal data, we will promptly report to the local authority and to the people (data subjects) involved.