V7 Ltd
158 Buckingham Palace Road
SW1W 9TR London, UK.

V7 - Short Data Security Statement

Data security has been central to V7 Darwin since early development, as our tools were set to host and operate on sensitive medical images and for deployment on the infrastructure of enterprises with strict security standards.

Terms of Service

As stated in Clause 5 ('Intellectual Property Rights and Use of Customer Data.') of our Terms of Service (https://www.v7labs.com/terms):

> **5.1 Intellectual Property Rights.** Except as expressly set forth in this Agreement, this Agreement does not grant either party any rights, implied or otherwise, to the other party's content or any of the other party's intellectual property. As between the parties, Customer owns all Intellectual Property Rights in Customer Data, and V7 owns all Intellectual Property Rights in the Services and Platform.
>
> **5.2 Use of Customer Data.** V7 will not access or use Customer Data, except as necessary to provide the Services and TSS to Customer.
>
> **5.3 Customer Feedback.** If Customer provides V7 Feedback about the Services, then V7 may use that information without obligation to Customer.

Customer (you, the reader) does not transfer ownership of any data loaded into our platform, nor does V7 have the right to access it if not to deliver the platform's services as requested by the user.

Storage of Data

Standard V7 Darwin accounts have their data stored on AWS S3 servers located in Ireland (EU). The use of Auto-Annotate and other deep-learning based tools will involve an AWS P2 instances located in the same region.

On-Premise and Private Cloud installations will depend on the customer's infrastructure location.

Third Party Access of Data

V7 **does not** mix, grant access to, or reveal any customer data to third parties unless explicitly instructed to by the customer.

Vulnerability and Penetration Testing

Vulnerabilities testing on the platform is performed quarterly, in addition to occasional ad-hoc vulnerability tests performed at customer requests. V7's team includes expertise in cybersecurity, cyberdefense, and penetration testing.

Additional Security Arrangements

- 2-factor authentication is enforced throughout our organisation
    - Only three individuals across V7 Ltd have admin access to our cloud infrastructure accounts.
- All V7 employees are restricted from using personal devices that contain known or suspected vulnerabilities or back-doors, including recording equipment, networking equipment, and mobile devices.
    - We periodically monitor whether any vulnerabilities are present within any software or hardware used on V7's machines or by employees.
- The third party services involved with the use of our tools are:
    - ScoutAPM - Used for monitoring server load.
    - AWS (owned by Amazon Inc) - Data is stored on S3 buckets and AWS P2 instances are used for deep learning applications.

Customer References by Location

Certain regions of the world have special arrangements for data security, we strive to respect these data security requirements and make continuous changes to adhere to local legislation:

Germany
Among our customers in Germany are Sartorius AG, Merck KGaA, and Miele GmbH, all three of which have had their legal team review our T&Cs and their technical team(s) review our current infrastructure setup.