Intetics Technical and Organisational Measures (TOMs) for Desk-Net Annex to the Data Protection Agreement between Desk-Net GmbH and Intetics sp. z o.o.

Physical Security

The Processor's delivery centers have personalized electronic key card access, video surveillance, fire alarm and physical intrusion detection systems.

Hardware Security

The Processor's computers have only one owner at any moment. Hardware maintenance is being done by qualified engineers only. All device content is encrypted. When a storage device is being passed from one person to another, wipeout procedure is mandatory.

Network Security

The Processor's local area networks are protected by firewalls. Internal network is split into VLANs. Public servers reside in isolated segments (DMZs). Offices are connected via encrypted VPN channels.

Information Systems Security

The Processor maintains a zero-trust security model which means that all laptops and workstations are protected at the same and the highest level of security, not looking on if it's an office or remote device.

The Processor uses a mobile device management system which enforces security policies on all information processing devices, including laptops, desktops, tablets and mobile phones.

The Processor implemented conditional access which permits the use of corporate systems only on approved and compliant devices. All non-registered and/or non-compliant devices are bounced even if the user credentials are correct.

The Processor's employees have individual passwords which are kept in secret and are changed every 6 months. All logins require 2-factor authentication to complete the login process.

Access rights to the information systems are granted after managers' approvals. Test and production environments are separated. All servers and workstations are regularly updated and have antivirus protection. Mission-critical information systems reside in a modern secure datacenter. Off-site backups are taken regularly.

Business Continuity

The Processor has Business Continuity plans which include all possible scenarios of natural and technogenic disasters. The plans are regularly tested and updated.

Secure Development

The Processor has a Secure development policy which requires the use of the industry-leading secure coding practices. Developers periodically pass trainings, participate in workshops and get certifications to improve their knowledge. Project managers are required to assess and mitigate risks in their everyday practices.

On behalf of **Controller**

Kretschmer

Name: Matthias Kretschmer

Title: CEO & Founder

Date: 01.01.2024

On behalf of **Processor**

Tomasz Baran

Name Tomasz Baran

Title: Member of the Board

Date: 01.01.2024

Signature Certificate

Reference number: SYAUT-JBYDR-Q3YLP-DCETK

Signer	Timestamp	Signature
Tomasz Baran Email: t.baran@intetics.com		
Sent:	20 Dec 2023 17:47:24 UTC	
Viewed:	21 Dec 2023 11:02:14 UTC	
Signed:	21 Dec 2023 11:02:43 UTC	
Recipient Verification:		IP address: 185.232.116.166
✔Email verified	21 Dec 2023 11:02:14 UTC	Location: Krakow, Poland

Document completed by all parties on:
21 Dec 2023 11:02:43 UTC