

Acceptable Use Policy

The following Acceptable Use Policy is valid from and last updated on the 18th of June, 2023.

Use of the Services is subject to this Acceptable Use Policy. You agree not to misuse the Services or help anyone else do so in ways described hereunder and understand liabilities that arise under the breach of this Acceptable Use Policy. Please note that capitalised terms have the meaning stated in the Terms of Service.

Misuse of the Services may be:

1. Service Disruption

1.1. Compromising the integrity, confidentiality and/or availability of our Services and/or systems of our Services, including our sub-processors' services and systems related to the delivery of our Services. This includes probing, scanning, or testing the vulnerability of any system or network that hosts our Services.

1.2. Tampering with, reverse-engineering our software, circumventing any security or authentication measures, or attempting to gain unauthorized access to the Services, related systems, networks, or data.

1.3. Overwhelming or attempting to overwhelm our infrastructure by imposing an unreasonably large load on our systems.

1.4. Deciphering any transmissions to or from the servers running the Services.

2. Service Misuse

2.1. Sending altered, deceptive or false source-identifying information, including "spoofing" or "phishing".

2.2. Disparaging us or our partners, vendors, or affiliates.

2.3. Promoting or advertising products or services other than your own without appropriate authorization.

2.4. Using the Services to violate the privacy of others, including the publishing or posting of other people's private and Confidential Information without their express permission, or collecting or gathering other people's Personal Data.

2.5. Sending authentication and/or signature request to multiple random recipients that do not expect the request and have not coordinated with the sending party accordingly.

2.6. The Services may only be used to store Customer Data that the User has lawfully obtained or created. The Services may not be used directly or indirectly for any illegal activity.

2.7. The Services may not be used for providing your own electronic identity security solution based on user authentication or signing operation performed using Dokobit API services. For example, a Customer logs in with any of our supported eIDs and in the same session, you ask the Customer to register a User using a self-chosen password that the Customer then uses in future authentications.

2.8. Dokobit API services that have been provided may only be used in the User's systems after a successful integration review by Dokobit. The provided API access may not be reused directly or indirectly in any other 3rd

party systems that were not included in the initial integration review. If the Services are to be used in the 3rd party systems, a new agreement with new access for each usage shall be provided.

2.9. Failing to ensure the ENISA-recommended level of security in the systems that integrate our Services (ENISA recommendations for algorithms, key sizes, and parameters).

2.10. Accessing or searching any part of the Services by any means other than our publicly supported interfaces (for example, "scraping").

3. Inappropriate content

3.1. Posting, uploading, sharing, submitting, or otherwise providing content that:

3.1.1. Infringes the Service Provider's or a third-party's Intellectual Property or other rights, including any copyright, trademark, patent, trade secret, moral rights, privacy rights of publicity, or any other Intellectual Property right or proprietary or contractual right;

3.1.2. Is pornographic, contains extreme acts of violence or terrorist activity, including terror propaganda, or is otherwise unlawful;

3.1.3. Advocates bigotry or hatred against any person or group of people based on their race, religion, ethnicity, sex, gender identity, sexual orientation, disability, or impairment;

3.1.4. Encourages illegal or tortious conduct;

3.1.5. Contains viruses, bots, worms, scripting exploits, or other similar materials;

3.1.6. You don't have the right to submit;

3.1.7. Could otherwise cause damage to the Service Provider or any third party.

4. Violation of Acceptable Use Policy

4.1. Violations by you, your company, or any other party authorized to access and use the Services may result in blocked access to or partial or full suspension of the Services or other reasonable actions appropriate to address the violation, as determined by us in our sole discretion.

4.2. We reserve the right to act without notice when necessary to preserve the stable, secure and uninterrupted operation of the Services, as determined by us in our sole discretion.

4.3. We may involve and will cooperate with law enforcement agencies and government agencies if criminal activity is suspected. Violators may also be subject to civil or criminal liability under applicable law.

4.4. In case of violation of this Acceptable Use Policy, the Customer shall not be entitled to any compensation.