Technical and Organisational Measures - TOM

Overview

In compliance with Article 32(1) of the GDPR, we provide the following Technical and Organisational Measures (TOM), describing the technical and organisational measures implemented by Landbot to ensure an appropriate security level.

Landbot uses Google Cloud Platform (GCP) as its cloud hosting provider for all the available environments, meaning that part of our technical security measures relies on Google's controls. For instance, all physical security restrictions are managed by Google in its data centers.

In contrast, Landbot must ensure the proper remote access and use of the information generated, protecting the data against intruders and external mischief as well as careless, inexpert, or unauthorized use.

Technical Measures

1. All instances are located in a reliable and certified Data Centre, **Google's servers in Belgium, Europe** (Google Cloud Engine, west-1). You can read more about Google's Security and Infrastructure in https://cloud.google.com/security/infrastructure/, and its compliance in https://cloud.google.com/security/compliance .

2. We have implemented access control tools based on authority levels and job functions.

3. Data is encrypted both at rest and in transit. We use TLS encryption to protect the data in transit. In the database customer's passwords are encrypted.

4. Backup and Restore of Data: we create daily backups with a retention period of 7 days, and it is protected using an individual encryption key

5. To ensure the availability of Landbot's stack, we have automatic alerts that send us notifications when any of the system's components fails.

6. To detect undesirable behavior, we use the combination of event monitoring and visualization software for controlling the stack used by Landbot.

7. We keep the data associated with your account until the User deletes the account's information or the account itself. That means we will hold the data for as long as the User has an account with us - while the Services are provided.

8. Landbot's platform deployment is entirely automated, and changes to both infrastructure and code are executed through our Continuous Integration (CI) and Continuous Delivery process (CD).

9. Our CI/CD process includes testing pools before releasing changes to any environment.

Organisational Measures

1. We regularly review our data privacy measures and policies to meet all the legal requirements.

2. Periodically, we check the software updates of the used components to process personal data. The patching is announced in https://status.landbot.io/ by creating a scheduled maintenance entry.

3. We conduct regular internal and external penetration tests and periodic scans, identify security vulnerabilities and remediate according to severity for any weakness found.

4. We have a written internal Business Continuity (BCP) and Disaster Recovery Plan (DRP) setting forth processes to restore the platform.

5. No less than once every six months, a contracted third party assesses our platform's security.

6. Our development process includes QA and code review by peers to ensure our releases' security, performance, and quality.

7. We have access removal processes to revoke access to staff who no longer need it.

8. We use a password manager and password generation solution to lock our passwords and personal information in a secure vault to protect our accounts.

9. Following the requirements covered in Articles 32-34 of the GDPR, we have procedures to create security breach reports and notify data subjects and regulators when needed.

10. Processes are in place to alert our team of any suspicious activity for review.