

## DATA SECURITY AND PROTECTION POLICY

### DEFINITIONS

WACG	means the WACG Inc., a company behind the Project Data Suite ( <a href="https://projectdata.io">projectdata.io</a> )
GDPR	means the General Data Protection Regulation.
Responsible person	means Oleg Snurnykov, a CTO, and a co-founder of the WACG inc.

### INTRODUCTION

At WACG we highly respect and value the data protection rights of our customers and partners.

The goal of this data protection policy is to depict the data protection aspects in one summarising document.

### DATA PROTECTION PRINCIPLES

WACG is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.”

### GENERAL PROVISIONS

1. This policy applies to all personal data processed by the WACG.
2. The Responsible Person shall take responsibility for the WACG’s ongoing compliance with this policy.
3. This policy shall be reviewed at least annually.

### LAWFUL, FAIR AND TRANSPARENT PROCESSING

1. To ensure its processing of data is lawful, fair and transparent, WACG shall maintain a Register of Systems.
2. The Register of Systems shall be reviewed at least annually.

3. Individuals have the right to access their personal data and any such requests made to the WACG shall be dealt with in a timely manner.

#### LAWFUL PURPOSES

1. All data processed by the WACG must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
2. The WACG shall note the appropriate lawful basis in the Register of Systems.
3. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
4. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the WACG's systems.

#### DATA MINIMISATION

The WACG shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

#### ACCURACY

1. The WACG shall take reasonable steps to ensure personal data is accurate.
2. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

#### ARCHIVING / REMOVAL

1. To ensure that personal data is kept for no longer than necessary, the WACG shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
2. The archiving policy shall consider what data should/must be retained, for how long, and why.

#### SECURITY

1. WACG shall ensure that all the data, including personal data, is stored securely using modern software and appropriate cloud services that are kept-up-to-date and compliant to regulations.
2. Data in transit shall be protected using transport level security technology.
3. Data in rest shall be protected with the appropriate encryption technologies.
4. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
5. WACG employees shall use multifactor authentication as a best practice and an industry standard.
6. When personal data is deleted this should be done safely such that the data is irrecoverable.
7. Appropriate back-up and disaster recovery solutions shall be in place.
8. WACG systems shall be cloud-based to the maximum possible extent, utilizing the best industry resources to maximize data security and protection at all levels.

#### BREACH

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data, the WACG shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach.