Privacy Statement

Regulation 45/2001 (herein after "the Regulation") applies to the processing of personal data carried out in the process of selection and recruitment of staff at Institution Nivo-Bio Kft.

Further to Article 11 and Article 12 of this Regulation, the Institution Nivo-Bio Kft. provides the data subjects with the following information:

- The controller is the Institution Nivo-Bio Kft.
  Person designated as being in charge of the processing operation: Mr. Sandor Koncz
  Email: office@nivo-bio.com
- The purpose of the processing is to build up professional contact with customers and provision of marketing materials to them from Nivo-Bio Kft.
- The categories of data collected and used for the processing operations are:
  - administrative data (contact details)
- The recipients of the data are:
  - the Director

The customers have the right of access and the right to rectify the data concerning him or her by contacting the person designated as being in charge of the processing operation. The right of rectification can only apply to factual data processed within the selection procedure. In addition, data related to the admissibility criteria can not be rectified after the closing date of submitting applications.

- The legal basis of the processing operation at stake is Art. 6. GDPR.
- The time limits for storing the data are the following:
  - until the customer requests data deletion, maximum 10 years
- The customers have the right to have recourse at any time to the director at office@nivo-bio.com and to the EDPS edps@edps.europa.eu

Data Protection Policy

Nivo-Bio Kft.

Last updated	03. March 2024.

Definitions

Organisation	means Nivo-Bio Kft. a company registered under number Cg.01-09-411497, Hungary.
DPA	means the Data Protection Act 2018 which implements the EU's General Data Protection Regulation.
Responsible Person	means Mr. Sandor Koncz, managing director
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Organisation.

1. Data protection principles

The Organisation is committed to processing data in accordance with its responsibilities under the DPA.
DPA requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. 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;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. 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;
e. 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 organisational measures required by the DPA in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2. General provisions

a. This policy applies to all personal data processed by the Organisation.
b. The Responsible Person shall take responsibility for the Organisation's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. The Organisation shall register with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Organisation shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the Organisation shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by the Organisation must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. The Organisation shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. 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 Organisation's systems.

5. Data minimisation

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

6. Accuracy

a. The Organisation shall take reasonable steps to ensure personal data is accurate.
b. 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.

7. Archiving / removal

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

8. Security

a. The Organisation shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. 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.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Organisation shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

END OF POLICY