FANO 有光科技 Labs

PERSONAL DATA (PRIVACY) PROTECTION POLICY

Statement of Policy and Purpose of Policy

1. **Fano Labs Limited** (the "**Employer" or "we**") is committed to ensuring that all personal information handled by us is processed according to legally compliant standards of data protection and data security.
2. The purpose of this policy is to help us achieve our data protection and data security aims by:
    - Notifying our staff of the types of personal information that we may hold about them and what we do with that information.
    - Ensuring staff understand our rules and the legal standards for handling personal information relating to staff and others.
    - Clarifying the responsibilities and duties of staff in respect of data protection and data security.
3. This is a statement of policy only and does not form part of your contract of employment. We may amend this policy at any time, in our absolute discretion.

Who is Responsible for Data Protection and Data Security?

1. Maintaining appropriate standards of data protection and data security is a collective task shared between **Fano Labs Limited** and you. This policy and the rules contained in it apply to all staff and agents of the Employer, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers (**Agents**).
2. The Board of Directors has overall responsibility for ensuring that all personal information is handled in compliance with the law and has appointed Data Protection Officer as the Data Protection Officer with day-to-day responsibility for data processing and data security.
3. All Agents have personal responsibility to ensure compliance with this policy, to handle all personal information consistently with the principles set out in this document and to ensure that measures are taken to protect data security. The Employer has a zero-tolerance policy of unauthorized disclosure of personal information.
4. Any breach of this policy will be taken seriously and may result in disciplinary action. The Privacy Commissioner's Office (PCO) may issue an enforcement notice to the person and the Employer, with intent to direct that wrongdoer to stop violating the data collection principles and take any necessary remedial action. Non-compliance with the PCO's enforcement notice is an offence and is liable to a fine or imprisonment. The victim who suffers damage, including injury to feelings, as a result of such violation may also be entitled to compensation from you through civil proceedings.
5. You may commit an offence if you disclose any personal information of a data subject obtained from the Employer without the Employer's consent with the intention to obtain gain in the form of money or other property, whether for your own benefit or that of another person, or to cause loss in the form of money or other property to the data subject. You will also commit an offence if you disclose, irrespective of your intent, any personal

information of a data subject obtained from the Employer without the Employer's consent and the disclosure causes psychological harm to the data subject. The maximum penalty for the offence is a fine of HK$1,000,000 and imprisonment for 5 years.

What personal information and activities are covered by this Policy?

This policy covers personal information:

1. which directly or indirectly relates to a living individual who can be identified either from that information in isolation or by reading it together with other information we possess;
2. that is stored electronically or on paper in a filing system;
3. in the form of statements of opinion as well as facts;
4. which relates to Agents (present, past or future) or to any other individual whose personal information the Employer handle or control; and
5. which we obtain, hold or store, organise, disclose or transfer, amend, retrieve, use, handle, process, transport or destroy.

What personal information do we process about agents and what do we do with it?

1. The Employer collects personal information about you which:
    a. you provide or we gather before or during your employment or engagement with us.
    b. is provided by third parties, such as references or information from suppliers or another party that we do business with.
    c. is in the public domain.
2. The types of personal information that we may collect, store and use about you include records relating to your:
    a. Home address and contact details as well as contact details of your next of kin and their contact details.
    b. Recruitment (including your application form or CV, any references received, details of your qualifications, letter of employment and employment agreement).
    c. Pay records, bank account details, passport or Hong Kong ID details, details of your taxes and any employment benefits such as pension and health insurance (including details of any claims made).
    d. Any sickness absence or medical information provided.
    e. Religious or philosophical beliefs (e.g. specific dietary or holiday requirements).
    f. Sexual orientation, where this is disclosed to us (e.g. through providing details of your spouse or partner for the administration of benefits).
    g. Telephone, email, internet, fax or instant messenger use.
    h. Performance and any disciplinary matters, grievances, complaints or concerns in which you are involved.
3. The Employer will use the personal information to carry out our business, to administer your employment or engagement and to deal with any problems or concerns you may have including:

4. The Employer confirms that for the purposes of the PERSONAL DATA (PRIVACY) ORDINANCE (the "Ordinance"), the Employer is a Data User of the personal information collected in connection with your employment. We maintain control over the collection, holding, processing or use of your personal information.
5. If you consider that any information held about you is inaccurate, you are entitled to request your line manager or the Data Protection Officer to make the necessary correction. If they are satisfied that the data are indeed inaccurate, they will make the necessary correction. However, if they do not agree that the information is inaccurate, they will note your comments and inform you in writing why such correction is not made.
6. We will take reasonable steps to ensure that your personal information is kept secure, as described later in this policy and in general, we will not disclose your personal information to others outside the Employer except in the following occasions / for the following purposes:
    a. You have consented to such disclosure; or
    b. for the administration of your employment and associated benefits e.g. to the providers of our pension or insurance schemes; or
    c. to comply with our legal obligations or assist in a criminal investigation or to seek legal or professional advice in relation to employment issues, which may involve disclosure to our lawyers, accountants or auditors and to legal and regulatory authorities;
    d. there is an applicable exemption provided under the Ordinance.
7. By providing your personal information to us, you consent to the use of your personal information (including any sensitive personal data) in accordance with this policy.

Data Protection Principles

Agents whose work involves using personal data relating to Agents or others must comply with this policy and with the six data protection principles set out below:

- **Principle 1: Data Collection Principle**
- **Principle 2: Accuracy & Retention Principle**
- **Principle 3: Data Use Principle**
- **Principle 4: Data Security Principle**
- **Principle 5: Openness Principle**
- **Principle 6: Data Access and Correction Principle**

Data Security

1. We must all protect personal information in our possession from being accessed, lost, deleted or damaged unlawfully or without proper authorisation through the use of data security measures.
2. Maintaining data security means making sure that:
    a. only people who are authorised to use the information can access it;
    b. information is accurate and suitable for the purpose for which it is processed; and

   c. authorised persons can access information if they need it for authorised purposes. Personal information therefore should not be stored on individual computers but instead on our central system.
3. By law, we must use procedures and technology to secure personal information throughout the period that we hold or control it, from obtaining to destroying the information.
4. Personal information must not be transferred to any person to process (e.g. while performing services for us on our behalf), unless that person has either agreed to comply with our data security procedures or we are satisfied that other adequate measures exist.
5. Security procedures include:
   a. **Physically securing information**. Any desk, cupboard or cabinet containing confidential information must be kept locked. Computers should be locked with a password or shut down when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others.
   b. **Controlling access to premises**. Agents should report to security if they see any unauthorized person in an entry-controlled area.
   c. **Telephone precautions**. Particular care must be taken by Agents who deal with telephone enquiries to avoid inappropriate disclosures. In particular:
   d. the identity of any telephone caller must be verified before any personal information is disclosed;
   e. if the caller's identity cannot be verified satisfactorily then they should be asked to put their request in writing;
   f. do not allow callers to pressure you into disclosing information. In case of any problems or uncertainty, contact the Data Protection Officer.
   g. **Methods of disposal**. Copies of personal information, whether on paper or on any physical storage device, must be physically destroyed when they are no longer necessary. Paper documents should be shredded and CDs or memory sticks or similar must be rendered permanently unreadable. This should be done every three months.

Subject Access Requests

1. By law, any data subject (including Agents) may make a formal request for information that the Employer hold about them, provided that certain conditions are met. The request must be made in writing. A fee is payable by the data subject for provision of this information. In some circumstances it may not be possible to release the information about the Subject to them e.g. if it contains personal information about another person.
2. Any member of staff who receives a written request should forward it to the Data Protection Officer immediately.

Classes of Transferee

The information that you have supplied to the Employer for the purpose of employment may be passed to the Employer's insurers, bankers, medical practitioners providing medical services, any relevant staff unions and provident fund managers.

FANO 有光科技 Labs

Questions about Data Protection

1. If you have any questions or concerns about this policy or any other matter relating to Data Protection then you should contact the Data Protection Officer.
2. Please refer to the Personal Information Collection Statement which should be provided to a job candidate to inform him/her how his/her personal information will be used, why the Employer collects them and what happens to his/her application if certain data is not provided.