TEN INTELLIGENCE LIMITED
PRIVACY NOTICE

1. Scope

Ten Intelligence Ltd ("**TenIntelligence**", "**we**, "**us**") respects the privacy and legal rights of the individuals and organisations we deal with.

TenIntelligence is a private company incorporated in England and Wales with company registration number 08134087 and registered address at 40 Churchill Square, Kings Hill, West Malling, Kent ME19 4YU.

Under the General Data Protection Regulation ("**GDPR**"), we now have to supply data subjects with Privacy Notices that contain significantly more information than they do under the Data Protection Act 1998. This is in order to meet new requirements about being transparent and providing accessible information to customers / individuals about how we are going to use their personal data so that they are fully informed and are aware of how they can exercise their rights under the GDPR.

2. Who are we?

TenIntelligence provides due diligence, litigation support and pre-employment screening services to or on behalf of our clients.

3. Description of our services ("Services")

Our due diligence services in respect of individuals assist our clients (or their clients) in complying with their legal obligations under statute or regulation to conduct due diligence in respect of certain individuals, e.g. anti-money laundering regulations, anti-bribery and corruption legislation as well as financial regulator and listing rules and regulations. In this regard we provide due diligence, background checks and screening in respect of current or proposed directors or investors of companies admitted to AIM, NEX Exchange or the Official List on behalf of their Nominated Advisors, as required by the applicable listing and/or regulatory rules. Our due diligence services are also requested by clients where it is in their commercial interest, e.g. fraud prevention and detection. We also assist with due diligence and checks on individuals for immigration purposes.

Our litigation support services provide essential information to assist our clients (or their clients) with current or prospective legal claims or proceedings or with fraud prevention, detection or investigations.

Pre-employment screening services entail background checks and executive screening on individuals at the request of the individual's current or future employer.

The due diligence and checks that are conducted as part of the Services include, without limitation, verification of current and previous employment, education, professional and technical qualifications, identity checks, address verifications, land registry checks, regulatory checks, financial checks, watchlist and sanctions database checks, corporate appointment history, civil ligation checks, criminal record checks as well as media, social media and internet searches.

Industry insight interviews and references are also requested from time to time. These checks are global, based on where the relevant individual has lived and worked in the past.

The actual scope of checks and screening done are dependent on the level of due diligence requested by our client.

4. Privacy notice

This Privacy Notice set outs details about the personal information we collect, process and hold in respect of individuals in the course of providing the Services.

TenIntelligence will be what is known as the "Controller" of the personal data provided to us in the course of providing the Services, although in some instances we may only act as the "Processor" of such personal data.

4.1 Description of personal data collected and processed in the course of providing the Services

The personal data that TenIntelligence may collect, hold and process about you in the course of providing the Services, are set out in Schedule 1. The personal data may be collected directly from you or indirectly via our client. We also obtain information from the following sources:

Current or Previous Employers	Professional Bodies/Associations	Court Records
Education Establishments	Criminal Record Agencies	Government Departments
Foreign Police Forces	Sanction & Watchlists	Regulatory Bodies
Corporate Registries	Online open source databases	Subscription databases (e.g. Lexis Nexis and Dow Jones)
Online Verification Services (HEDD, Student Clearing House)	Third party human source intelligence (insights and references)	Land Registries
Electoral Registers	Address and Telephone Directories	Internet searches
Media sources	Site visits	Surveillance

However, not all the data set out in Schedule 1 may be collected and processed about you and not all the sources above will necessarily be utilised – the level of personal data collected or processed and the sources used may vary from case to case and will depend on the scope of the Services requested by our client.

The personal data we collect or process about you may include those defined as "Sensitive Personal Data" as well as criminal conviction data. Sensitive Personal Data includes racial or ethnic origin, political opinions, religious beliefs, membership of trade union, physical and mental health and sexual life or orientation.

We will not collect, process or hold any personal data about you that we do not need in order to provide the Services to our client.

4.2 **Why do we need this personal information– legal basis of processing**

The legal basis on which we collect, hold and process your personal information is the **legitimate interests of our clients**, as follows:

- The client's legal obligation under statute or regulation to conduct due diligence or background checks on individuals;
- The client's commercial interest to detect or prevent fraud;
- The client's commercial interest to conduct executive screening and pre-employment or appointment verifications;
- The client's commercial interest to conduct due diligence as part of their client on-boarding process, supply chain screening and vetting of parties prior to prospective investments or transaction;
- The client's commercial interests to establish, exercise or defend legal claims/rights or to obtain legal advice or insofar as it relates to any current or prospective legal proceedings in respect of the client;
- The client's obligation to maintain effective immigration controls.

Our legal basis for processing Sensitive Personal Data and Criminal Conviction Data are as follows:

Data	**Purpose**	**Legal Basis**
Sensitive Personal Data	Due Diligence	(1) Legitimate interests (2) Substantial Public Interest (Preventing Fraud or Protecting the Public against dishonesty etc)
Sensitive Personal Data	Litigation Support	(1) Legitimate interests (2) Court Action & Legal Claims (3) Substantial Public Interest (Preventing or detecting unlawful acts)
Sensitive Personal Data	Pre-employment Screening	(1) Legitimate Interests (2) Substantial Public Interests – Preventing Fraud
Criminal Conviction Data	Due Diligence	(1) Legitimate Interests (2) Substantial Public Interest (Preventing Fraud, Preventing or Detecting Unlawful Acts or Protecting the public against dishonesty etc)
Criminal Conviction Data	Litigation Support	(1) Legitimate Interests (2) Specific Legal Authorisation (Legal Claims) (3) Substantial Public Interest (Preventing or detecting unlawful acts)
Criminal Conviction Data	Pre-employment Screening	(1) Legitimate Interests (2) Substantial Public Interest (Preventing Fraud)

4.3 **What we do with the personal information?**

All the personal information we hold about you will be processed by our staff in the United Kingdom.

We will not share your personal information with third parties for purposes other than the provision of the Services. In some cases, we may share your personal information with our affiliated companies, agents, suppliers, clients, or with third party service providers retained by us to provide the Services on our behalf. These parties will use your personal information only to accomplish the provision of the Services.

We may also share your personal information with previous employers, colleagues or educational or professional institutions for purposes of employment, membership or education verifications or the provision of references.

We take all reasonable steps to ensure that your personal data is shared and processed securely and confidentially.

Your personal information may also be shared under the following circumstances: (i) if we are required to do so by law enforcement authorities or government agencies or for other regulatory purposes; and (ii) in connection with investigations or other efforts to prevent illegal activities or pertaining to public safety.

We may disclose and transfer your personal information during a merger or during the divestiture of company assets. However, we will require the acquiring organization to agree to protect the privacy of your personal information in accordance with this privacy notice.

4.4 **Transfer of Personal Information outside the European Economic Area (EEA)**

As mentioned earlier, the due diligence, pre-employment screening and litigation support services we provide are global and, in this regard, we may be required to transfer your personal data outside the EEA for purposes of the provision of the Services.

Such transfers will be protected by the following safeguards, as may be appropriate:

- The European Commission has made an "adequacy decision" with respect to the data protection laws of the relevant jurisdiction or country to which the data is transferred;
- Transfers are protected by the use of standard data protection clauses adopted or approved by the European Commission;
- Transfers are protected by the US Privacy Shield.

Transfers may also be made where it is necessary for the performance of a contract made in your interest between us and our client, for example, the obtaining of verifications in countries outside the EEA for your benefit.

If you require specific information about any transfers of your personal data and specific safeguards that may apply, please contact us at dpo@tenintel.com.

4.5 **Retention period**

We will destroy most of the personal information we hold about you within 3 months of conclusion of the provision of the Services to our client, unless we are required by law to retain it for a longer period.

A copy of the report containing your personal information as provided to our client will be retained on our systems For a minimum of 1 year up to 6 years after which time it will be destroyed according to our destruction process if it is no longer required for the lawful purpose(s) for which it was obtained.

For further information about our data retention policy and schedule, please contact dpo@tenintel.com.

4.6 **Your rights as a data subject**

At any point while we are in possession of or processing your personal data, you, the data subject, have the following rights:

- Right of access – you have the right to request a copy of the information that we hold about you free of charge. However, please note that we may charge a reasonable fee when your request is manifestly unfounded, excessive or repetitive.
- Right of rectification – you have a right to correct data that we hold about you that is inaccurate or incomplete.
- Right to be forgotten – in certain circumstances you can ask for the data we hold about you to be erased from our records.
- Right to restriction of processing – where certain conditions apply you have a right to restrict the processing.
- Right of portability – you have the right to have the data we hold about you transferred to another organisation.
- Right to object – you have the right to object to certain types of processing such as direct marketing.
- Right to object to automated processing, including profiling – you also have the right to be subject to the legal effects of automated processing or profiling.

In the event that TenIntelligence refuses your request under rights of access, we will provide you with a reason as to why, which you will have a right to legally challenge.
TenIntelligence at your request can confirm what information it holds about you and how it is processed.

You can request the following information:

- Identity and the contact details of the person or organisation that has determined how and why to process your data.
- Contact details of the data protection officer, where applicable.
- The purpose of the processing as well as the legal basis for processing.
- If the processing is based on the legitimate interests of TenIntelligence or a third party, information about those interests.
- The categories of personal data collected, stored and processed.
- Recipient(s) or categories of recipients that the data is/will be disclosed to.

- How long the data will be stored.
- Details of your rights to correct, erase, restrict or object to such processing.
- How to lodge a complaint with the supervisory authority (ICO).
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether you are obliged to provide the personal data and the possible consequences of failing to provide such data.
- The source of personal data if it wasn't collected directly from you.

To access what personal data is held, identification will be required

TenIntelligence will accept the following forms of ID when information on your personal data is requested: a copy of your driving licence, passport, birth certificate and a utility bill not older than three months. A minimum of one piece of photographic ID listed above and a supporting document is required. If TenIntelligence is dissatisfied with the quality, further information may be sought before personal data can be released.

All requests should be made to dpo@tenintel.com or by phoning +44 (0) 203 963 1930 or writing to us at The Data Protection Officer, Ten Intelligence Limited, 40 Churchill Square, Kings Hill ME19 4YU.

4.7 **Complaints**

If you wish to raise a complaint about how we have handled your personal data, including in relation to any of the rights outlined above, you can contact our Data Protection Officer at dpo@tenintel.com or by phoning +44 (0) 203 963 1930 or by post at The Data Protection Officer, Ten Intelligence Limited, 40 Churchill Square, Kings Hill ME19 4YU, who will investigate your concerns.

If you do not get a response within 30 days, or if you are not satisfied with our response, or believe we are processing your data unfairly or unlawfully, you can complain to the Information Commissioner's Office (ICO) at 0303 123 1113. You can find further information about the ICO and their complaints procedure here: https://ico.org.uk/concerns/.

SCHEDULE 1

Data Obtained
Full Name and Surname
Date of Birth
Gender
Aliases
Address history for up to 10 years
Email
Mobile/landline numbers
Education details
Employment details (current and past)
Curriculum Vitae
Professional Qualifications and Registrations
Land Registry
Electoral Register
Work/Residence Permits
Litigation, dispute, CCJ and Bankruptcy Details
Credit History
Asset ownership
Corporate Registries details
Passport Details (including copy)
Driving Licence Details (including copy)
Utility Bills (including copy)
Photographic images
Professional References/Industry Insights
NI Number/Social Security Number
Identity Numbers
Social Media
Media
Public Profile
Financial history and information
Details of family members
Special category Data (Race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, sexual orientation)
Criminal Record Details