TRUE DILIGENCE
INDEPENDENT, ETHICAL AND TRANSPARENT

Data Protection Policy

True Diligence Limited
15 Old Bailey
London, EC4M 7EF

Last Updated: 30 December 2015

t: +44 (0) 203 397 8958
f: +44 (0) 203 397 9260
e: contact@truediligence.uk
w: www.truediligence.uk

DATA PROTECTION POLICY

INTRODUCTION

1. We recognise that everyone has rights with regard to how their personal information is handled. During the course of our business activities we will collect, store and process personal information about our staff, customers, suppliers and other third parties. We recognise the need to treat it in an appropriate and lawful manner.

2. We will routinely make our customers, suppliers and third parties aware of this policy. This is because we consider that data protection compliance is fundamental to our businesses success.

3. We seek to comply with the provisions of the Data Protection Act 1998. But we will go beyond that. We will seek to act in such a way that enhances the protection of data generally. This means that will seek to operate beyond what is required of us. We will work with our third parties on ways that we can do this.

DATA PROTECTION PRINCIPLES

4. Anyone processing data (including us) must comply with the eight enforceable data protection principles, which are laid out in the Data Protection Act 1998 ("DPA" or "the Act") and the website of the Information Commissioners' Office. The principles provide that data must be:

    4.1. processed fairly and lawfully;

    4.2. processed for limited purposes and in an appropriate way;

    4.3. adequate, relevant and not excessive for the purpose;

    4.4. accurate;

    4.5. not kept longer than necessary for the purpose;

4.6. processed in line with data subjects' rights;

4.7. secure.

4.8. not transferred to people or organisations situated in countries without adequate protection.

FAIR AND LAWFUL PROCESSING

5. The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case, it is True Diligence Limited), the purpose for which the data is to be processed, and the identities of anyone to whom the data may be disclosed or transferred.

6. For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed.

PROCESSING FOR LIMITED PURPOSES

7. Personal data will only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data will not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject will be informed of the new purpose before any processing occurs.

ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

8. Personal data will only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose will not be collected in the first place.

ACCURATE DATA

9. Personal data will be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps will therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data will be destroyed in line with our policy decisions on data retention.

10. We may use databases and systems which will automatically correct data that is incorrect. It might also flag up data that appears to be incorrect or out of date. We may at this stage decide if we ought to correct the data, or destroy it.

DATA RETENTION

11. Personal data will not be kept on our systems longer than is necessary. This means that data must be erased from our systems after a period of time has elapsed. We call this period of time a 'retention period'.

12. Sometimes, the retention period may be a very short period of time, such as couple of days or weeks. However, it may be that on occasions, we are required to keep information for a lot longer - such as several years and as such, the retention period will reflect that.

13. For example, where we are asked to verify an address for a director of a company using information that we have been provided, we may retain the information long enough for us to perform our own electronic enquiries and, once we have verified it, erase all of the other information. That is because we have carried out our function and the retention of the data is unlikely to be of any value to us. In another example, where we perform physical surveillance in support of a fraud investigation, we may keep the surveillance imagery up until a prosecution is commenced, or where disciplinary action is taken, or where we are told that no further action will be taken.

PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

14. Data will be processed in line with data subjects' rights. Data subjects have a right to:

14.1. request access to any data held about them by a data controller.

14.2. prevent the processing of their data for direct-marketing purposes.

14.3. ask to have inaccurate data amended.

14.4. prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else.

14.5. object to any decision that significantly affects them being taken solely by a computer or other automated process.

DATA SECURITY

15. We will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

SUBJECT ACCESS REQUESTS

16. A formal request from a data subject for information that we hold about them must be made in writing. A fee of £10 is payable by the data subject for provision of this information. We will comply with subject access requests in the time allowed by the Data Protection Act 1998 however, we will do our best to comply as quickly as possible.

17. We reserve the right to request further information before carrying out our request, such as the provision of identification documents. However, we will not act unreasonably and will comply with the spirit of the Data Protection Act 1998, as well as the requirements of it.

THIRD PARTY DATA

18. Because of the nature of the work we do (due diligence investigations), we subscribe to a number of third party databases. These databases compile data from a range of different sources. For example, we subscribe to third party databases that compile: electoral roll data, directorship data, county court judgment data, previous address information, deceased data, insolvency data and demographic data. This information is generally available in the public domain however, it might be that a fee is charged to access such data (such as the case with Registry Trust for County Court Judgment data).

19. We rely on third parties to provide us with data that is reliable. However, on occasions, they may get it wrong. We will work with our third parties to manage these potential exposures.

CRIME DETECTION AND PREVENTION

20. Because of the nature of the work we do, we do process, obtain and disclose information for the purposes of the detection and prevention.

HOW TO COMPLAIN

21. If you have a complaint about the way we have handled, processed, obtained or otherwise engaged with your personal data, we'd ask that you follow our complaints policy. We will treat complaints of this nature with the utmost urgency to ensure a prompt, fair and satisfactory outcome for all of those concerned.

22. If you believe that we have breached the Act, please let us know immediately by telephone on 0203 397 8958 or via e-mail at complaints@truediligence.uk. This is so that we can work immediately to rectify the problem. We will reward those who assist us identifying breaches of the Act.

23. The Information Commissioners Office will expect you to complain to us in the first place, rather than go directly to the ICO. Irrespective of that, we will still treat your request with the seriousness that it deserves if you prepare a complaint.