CJ Property Cleaning LTD
Policy Document
Data Protection Policy
27.11.2020

DATA PROTECTION POLICY

Introduction

Anyone who obtains personal information ("data") about other individuals is a 'data controller' and is thus regulated by the Data Protection Act 1998. The Act controls what can lawfully be done with information.

It also gives individuals certain rights to control how information about them is obtained, used, stored and distributed. These rights include the right to find out what information a data controller has about them, and to ask for copies of data.

The company is necessarily a data controller in relation to all the information that it obtains about its employees as part of the process of providing them with employment.

In order to manage company business, employees' records are kept that are necessary and include the following information:

- Name.
- Date of birth.
- Gender.
- Address.
- Next of kin.
- Sickness record.
- Disciplinary record.
- CV.
- References.
- Qualifications.
- Rate of pay.

- Bank details.
- Performance record.
- Appraisals.
- Criminal records.

It is a requirement under the Act that the company obtains employees' consent to the storage and processing of data about them. Some data is referred to in the Act as "sensitive personal data". This means personal data consisting of information as to:

- The racial or ethnic origin of the data subject.
- His/her political opinions.
- His/her religious beliefs or other beliefs of a similar nature.
- Whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992).
- His/her physical or mental health or condition.
- His/her sexual life.
- The commission or alleged commission by him/her of any offence.

Or:

- Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings, or the sentence of any court in such proceedings.

The company requires that employees express consent in their contracts of employment to the processing of their sensitive and other personal data. Without this consent it is not necessarily lawful for the company to process data in order to keep the employment records necessary for us to run our business.

Below is a summary of the legal obligations imposed upon the company and the rights that employees have under the Data Protection Act 1998 together with the company's policies about those rights and obligations. The Act contains transition periods under which its terms become fully effective over a period of years, however company policy assumes that the Act is fully in force.

The company's obligations

The principles for processing of personal data are that data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to countries without adequate protection.

The company is committed to following these principles and that is why your consent is sought so that all company data processing in relation to employees is lawful.

The company will process data about employees only as far as is necessary for the purpose of managing its business. Data will not be disclosed to anyone else other than the company's authorised employees, agents, contractors or advisors (except as required by law) unless such disclosure is expressly authorised. The company will only obtain data that is required for the purpose of managing its business and dealing with its employees.

The company will take all reasonable steps to ensure that the data it stores, and processes, is accurate. Data will be retained all through periods of employment and records will be retained for up to six years after the date that employment ceases in case legal proceedings arise during that period. Data will only be retained for a period of longer than six years if it is material to legal proceedings, or should otherwise be retained in the company's interests after that period.

The company will process data in accordance with employees' rights under the Act.

Data will be kept in a secure system whether manual or computerised to the best of the company's ability at all times.

The Act prohibits the transfer of data outside the European Economic area to countries that do not have similar protection of data except in some circumstances or with the subject's consent. Employees' contracts of employment embody consent to such transfers should they be necessary. The reason for this is that with the use of the Internet, and email, data can be transferred to a computer or server in such a country in the course of a transfer between parties within the European Economic area. Also the company may have offices or subsidiary companies or agents or contractors in such countries now, or in the future, and therefore transfers of data could be necessary as part of the management of its business and the activities of its employees.

Your rights under the Act

The Act gives the following rights to data subjects:

- Access to data

    - To be told whether and which personal data is being processed by requesting this in writing and paying a fee currently not to exceed £10.00.

    - To be given a description of the data and its recipients and to have a **copy** of the data within 40 days of the request. Confidential references given **by** the company are excluded from disclosure (but not necessarily references given ***to*** the company). The data subject is entitled to know the source of the data.

    - The copy should be intelligible and in a permanent form unless to provide it in this form is impossible, or would involve disproportionate effort, or if it is agreed that an impermanent "copy" is acceptable.

    - If the data controller has previously complied with a request from an employee then no duty to comply with another request arises until a "reasonable interval" has elapsed between the two. Just what will constitute a "reasonable interval" will depend on the nature of the data, why it is processed and the frequency with which it alters.

    - To be informed about the logic used to make automated decisions using the data. For example, some employers will scan CVs submitted for certain information in order to select candidates for further consideration and this right would entitle the candidate to know what the criteria used was unless this would necessitate divulgence of a trade secret.

    - The request for access to data must be made in writing if the data controller so requires. The Data controller may also require payment of a fee not exceeding the statutory maximum which is currently £10.00.The data subject must provide the data controller with any information reasonably requested to enable the data controller to be satisfied as to the data subject's identity and in order to locate the information.

    - Where disclosure of data would necessarily mean that information relating to a third party would be disclosed, the data controller may refuse to disclose it unless the third party consents or it is reasonable to disclose the information without such consent.

- Rectification of data

Individuals can apply to a court for an order that the data controller rectify, block, erase or destroy inaccurate data and where the court considers it reasonably

practicable to do so inform third parties to whom the data has been disclosed of the fact.

- Compensation

Should an individual suffer damage as a result of the failure of a data controller to comply with the Act then he, or she, may be awarded compensation. Where a data subject suffers distress in certain types of case there may also be an award of compensation for distress as well as damage.

It is a defence in any claim for compensation that the data controller used such care as was reasonably required in all the circumstances to comply with the Act.

- Information

The Act provides that data will not be fairly processed unless the data controller ensures that as far as reasonably practicable the data subject has or has ready access to:

- The identity of the data controller.
- Any representative of the data controller.
- The purpose(s) for which the data is intended to be processed.
- Any other information necessary to enable the processing to be fair.

The company has incorporated this information into its contracts of employment or otherwise given notice of this information (including this policy).

However any data subject whose employer has not notified the Office of the Information Controller that he/she is a data controller, and had these details entered in the public register, is entitled to be given (within 21 days of making a written request) "relevant particulars" which are:

- The data controller's name and address.
- The name and address of any representative of the data controller.
- A description of the personal data being or to be processed and the category of data subjects to which they relate.
- A description of the intended purpose of the processing.
- A description of the intended recipients of the data.
- A list of the countries outside the European Economic area that will or may be in receipt of the data from the data controller.

- Direct Marketing

A data subject has the right to require in writing that the data controller, within a reasonable time, cease or not begin processing data, of which he/she is the subject for the purpose of direct marketing. Failure to comply by the data controller can lead to a court order that he/she does so.

- Right to stop data processing

A data subject has the right to require that a data controller cease, or not begin, data processing where the processing is causing or likely to cause unwarranted and substantial damage, or unwarranted and substantial distress, to the data subject, or another, by giving notice in writing specifying why the data processing is or will be the cause of distress or damage and the purpose and manner of processing to which objection is made. The data controller then has 21 days to respond with a written notice stating either that he/she has or intends to comply with the request, or why he/she regards the notice as unjustified and the extent to which he/she has or intends to comply with it. The data subject can make an application to the court if the data controller will not comply. However where the data subject has consented to the data processing or it is necessary for the performance of a contract to which he/she is a party he requests it with a view to entering a contract, or the data controller has a non-contractual legal obligation which requires him to carry it out, the data subject has no right under this section to stop the data processing.

Company policy on access to data

- The company will appoint a data protection compliance officer.
- A request for access to any personal data should be made by a written request using the company's Data Access Request form which may be obtained from the company or after you have left employment by request to the data protection compliance officer at head office. While you remain in the employ of the company, no fee is payable, but post-employment a fee of £10.00 or such higher amount as permitted by law from time to time must be paid before access can be granted. The completed form must be returned to the data protection compliance officer with the fee if applicable.
- On receipt of a request it is company policy to provide copies of all data that the company is obliged to disclose within 40 days of receipt of your request being received by the data protection compliance officer at head office.
- The company considers that if a period of less than one year has elapsed since any previous request for access to data was complied with, it is not reasonable to expect the company to be obliged to comply with a further request before a year has elapsed - unless there are exceptional circumstances.
- Should an employee wish to bring any inaccuracy in disclosed data to the company's attention, this must be done in writing. In appropriate circumstances it may be that arranging an appointment to hand the company a written notification of any inaccurate data is preferable.

- It is company policy to ensure that all data is as accurate as possible and all necessary steps to ensure that this is the case and to rectify any inaccuracies will be taken.

Where the company has requested a reference in confidence from a referee, and that reference has been given on terms that it is confidential, and that the person giving it wishes that it should not to be disclosed to its subject, it is company policy that it would normally be unreasonable to disclose such a reference unless the consent of the person who gave the reference is obtained.