



ALBANY PARTNERS PRIVACY STATEMENT

Introduction

Purpose

Albany Partners Limited "Albany Partners" is registered in England, Company Number 08132209.

It is committed to being transparent about how it collects and uses the personal data of all individuals that it comes into contact within the course of its business, and to meeting its data protection obligations. This policy sets out Albany Partners' commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of potential candidates and candidates, referees, client contacts and other individuals that it comes into contact within the search process, referred to below as 'search-related personal data'.

Albany Partners has appointed James Goodrich, CEO & Founder, as the person with responsibility for data protection compliance within the organisation. He can be contacted at james@albanypartners.co.uk. Questions about this policy, or requests for further information, should be directed to him.

Definitions

"Personal data" is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

Albany Partners processes search-related personal data in accordance with the following data protection principles:

- Albany Partners processes personal data lawfully, fairly and in a transparent manner.
- Albany Partners collects personal data only for specified, explicit and legitimate purposes.
- Albany Partners processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Albany Partners keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- Albany Partners keeps personal data only for the period necessary for processing.
- Albany Partners adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Albany Partners tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where Albany Partners processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

Albany Partners will update search-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the search process is held securely and confidentially in hard copy or electronic format, or both, and on our case management and other IT systems (including email). The periods for which Partners holds search-related personal data are contained in its privacy notices to individuals.

Albany Partners keeps a record of its processing activities in respect of search-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, Albany Partners will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

Albany Partners will also provide the individual with a copy of the personal data undergoing processing upon request. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

To make a subject access request, the individual should send the request to James Goodrich at james@albanypartners.co.uk. In some cases, Albany Partners may need to ask for proof of identification before the request can be processed. Albany Partners will inform the individual if it needs to verify his/her identity and the documents it requires.

Albany Partners will normally respond to a request within a period of one month from the date it is received. In some cases, such as where Albany Partners processes large amounts of the individual's data, it may respond within three months of the date the request is received. Albany Partners will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, Albany Partners is not obliged to comply with it. Alternatively, Albany Partners can agree to respond but will

charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which Albany Partners has already responded. If an individual submits a request that is unfounded or excessive, Albany Partners will notify him/her that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require Albany Partners to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override Albany Partners' legitimate grounds for processing data (where Albany Partners relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override Albany Partner's legitimate grounds for processing data.

To ask Albany Partners to take any of these steps, the individual should send the request to James Goodrich at james@albanypartners.co.uk

Data security

Albany Partners takes the security of search-related personal data seriously. Albany Partners has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where Albany Partners engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Impact assessments

Some of the processing that Albany Partners carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, Albany Partners will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

If Albany Partners discovers that there has been a breach of search-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. Albany Partners will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

Albany will only transfer data to countries outside the European Economic Area (EEA) for the purposes of processing it on cloud based IT and case management systems. Data is transferred outside the EEA in accordance with the conditions set out in the GDPR and only to countries that have been certified by the European Commission as having an adequate level of data protection in place.

Individual responsibilities

Individuals are responsible for helping Albany Partners keep their personal data up to date, particularly as individuals will be the source of much of the personal data that Albany Partners holds.

Albany Partners staff may have access to the personal data of other individuals, including candidates, clients and referees, in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, Albany Partners relies on individuals to help meet its data protection obligations to those other individuals.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes in accordance with a legitimate business requirement;
- not to disclose data except to individuals (whether inside or outside Albany Partners) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from Albany Partners' premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under Albany Partners' disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing candidate or client data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

Albany Partners will provide training to all staff about their data protection responsibilities at regular intervals.

Website Data Collection Information

Note: 'Us' refers to Albany Partners 'You', 'User(s)', 'Visitor' refers to any person who uses this website.

Our web site www.albanypartners.co.uk is owned and controlled by Albany Partners Limited. Albany Partners is committed to implementing measures designed to protect the privacy of those using our services.

Albany Partners respects the privacy of all those who visit our site and use our online services and we collect information from and about our users to be used to improve the service we offer. Except as set forth within this Privacy Policy, our Terms & Conditions, and other published guidelines, we do not release personally identifiable information (as described below) about users of this site without their permission.

This Privacy Statement governs your interaction with this site, and your registration for and use of Albany Partners online services.

Opt-Out Option

If you would like to have your personally identifiable information removed from Albany Partners databases going forward, please email james@albanypartners.co.uk and we will use reasonable efforts to comply with your request. However, there will be residual information that will remain within Albany Partners website databases, access logs, and other historical internal records, which may or may not contain such personally identifiable information.

The information we may gather from your usage of this website:

1. Non-personally-identifiable information:

1.1 As a standard practice, Albany Partners assigns a random number to each user for anonymously tracking content preferences and traffic patterns. This random number lets us keep track of "how many" times users are doing specific things – like visiting our site each month – without really knowing who those users are (unless they specifically tell us). We analyse this data for trends and statistics, such as which parts of our site users are visiting and how long they spend there. We also gather information about what users are searching for. We use all this information in order to improve our content, plan site enhancements, and measure overall site effectiveness.

2. Personally identifiable information:

2.1 General: In certain areas of this site, we may require that you provide us with personally-identifiable information, in order to be able to use that portion or those portions of this site.

2.2 If you submit a request for more information from us, the information you submit will only be used by Albany Partners. Our lists are private and are never sold to any third parties. If you have any queries about this policy please feel free to contact us.

Information about Cookies

Cookies are text files placed on your computer to collect standard internet log information and visitor behaviour information. This information is used to track visitor use of the website and to compile statistical reports on website activity. Cookies act as a memory for a website,

allowing that website to remember your computer on your return visits. This is particularly important for websites that require you to sign in as it speeds up your access. We use both session cookies (which exist only until you close your web browser) and persistent cookies (which exist for a longer, specified period of time). The majority of web browsers accept cookies, but you can usually change the web browser's settings to refuse new cookies, disable existing ones or simply let you know when new ones are sent to your hard disk. However, please be aware that, if you refuse or disable cookies, some of the website's functionality may be lost. If you want to delete any cookies that are already on your computer, please refer to the instructions for your file management software to locate the file or directory that stores cookies. If you want to stop cookies being stored on your computer in future, please refer to your browser manufacturer's instructions by clicking 'Help' in your browser menu. However, some of our website features may not function as a result.