

## TERMS OF BUSINESS – CORPORATE

1. **Regulation.** We, advo group limited, of advo house, St Leonards Road, Maidstone, Kent, ME16 0LS are authorised and regulated by the Financial Conduct Authority (FCA) to sell general insurance products. Our FCA registered number is 308874 and you can check this on the FCA's register by visiting the FCA's website [www.fca.org.uk/firms/financial-services-register](http://www.fca.org.uk/firms/financial-services-register) or by contacting the FCA on 0800 111 6768.

2. **Our service to you.** In arranging insurance for our customers we act as an independent intermediary and act on your behalf when arranging your insurance. Our service includes: advising you on your company health and protection insurance needs; arranging insurance cover with insurers to meet your companies requirements; helping you with any ongoing mid-term adjustments you have to make and assisting with the renewal of insurance and employee benefit policies.

We offer a range of health insurance and protection products and have access to a number of insurers with whom we place insurance. We will give you details of these insurers when we discuss your requirements. We also offer a range of other employee benefits and work with other providers of benefits. We will give you details of these providers when we discuss your requirements.

3. **Personal Data.** The personal data we hold about your employees and their dependants includes their names, dates of birth, gender, marital status, home addresses and premium information. We also hold employees National Insurance numbers, company information such as work e-mail address, mobile number, start date, job titles, payroll number, cost centre, job grade or manager. We hold insurer documentation such as quotes which include details of your employees. We may also hold salaries, bonus payments, pension contributions, travel allowances, childcare vouchers, cycle to work, company car information, give as you earn and season ticket information.

4. **Data Processor and Data Controller.** In most instances we are data processors as we process the data on behalf of insurance companies and other providers of Health, Risk and Wellbeing products. There may be occasions when we become a Data Controller – this is where we determine the purpose for which and the manner in which any personal data is processed. An example of this might be when using our online platform for products or policies where we only hold the data. We are registered with the ICO under registration reference Z7559664.

5. **Sensitive Personal Data.** We may hold Sensitive Personal Data which includes health information in relation to risk products (such as Life and Income Protection policies), Private Medical Insurance, employee benefit programmes, Travel and Dental policies and other such medical and employee benefits. The purpose for holding health data is to be able to assist employees with claims queries. The individual employees will have consented to us having this sensitive information about them.

6. **Legal Basis.** Our lawful basis for processing personal data is that it is necessary for the performance of the broking contract which involves scoping and placing cover for Private Medical, Protection and other health insurance policies.

## TERMS OF BUSINESS – CORPORATE - PAGE 2.

6. **Legal Basis** *continued*. In order to obtain quotes for company policies, which include its employees, we must provide personal details of those employees, for example salary for a Life insurance policy or date of birth for a Private Medical Insurance policy.
7. **Claims Assistance**. We will never discuss a claim with anyone apart from the person who has made the claim or their representative, in the case of children or those who are unable due to ill health to speak with us, and a named contact at the insurance company or other employee benefit provider. We will obtain explicit consent from the claimant to share this information.
8. **Consent**. There may be occasions when we will require consent from your employees in respect of recording and managing Sensitive Personal Data. Our conditions for obtaining consent is that the employee has given us explicit consent to processing their information.

We will ask the employee to complete a consent form which we will stored on our systems.

9. **Authentication**. In order to authenticate an employee when they telephone advo group we will ask three data protection security questions to establish their identity. We will also ask three data protection security questions to Group Secretaries or others asking for information about a company's policy to ascertain they have authority to act on the company's behalf, and are a contact we can speak with.

We also have in place identification procedures when we contact insurance companies and other benefit providers.

10. **Who handles your employees Personal and Personal Sensitive information?** Each group policy has a dedicated Account Manager and Administrator who have access to your employee's data. On some larger corporate schemes there may be two Account Managers and one administrator in order to maintain service levels. You will be notified of your Account Manager(s) and Administrator at the start of your policy. There may be occasions when the Account Manager(s) and/ administrators will change and you will be notified of this change and introduced to your new contacts.

Access to your employee's personal and sensitive personal details is restricted on our system by a verification process. There may be occasions when another Account Manager or Administrator will need access to your employees' details, for example to cover holiday or sickness. In these instances, they must go through the verification process which is monitored.

11. **Storage**. Data is stored locally on advo systems and authentication solutions are required for access. All sensitive data is encrypted in traffic and at rest using Transparent Data Encryption (TDE) technology.

## TERMS OF BUSINESS – CORPORATE - PAGE 3.

12. **Safeguards.** All staff and contractors must sign confidentiality agreements and undergo criminal background checks prior to joining or providing services to advo. There is mandatory training on privacy and security awareness included in the induction process for all staff. This training is also given to all staff on an annual basis to make sure they are up to date. Staff are given their own customers and are identified on the system. There is also inbuilt security on the system which gives staff different levels of access to data so that staff only have access to their own customer's policies.
13. **Information Security.** All data stored on staff computers requires strong passwords to access data. If laptops are lost or stolen, data confidentiality and integrity are not at risk, data can be wiped ensuring confidentiality and integrity are maintained.

Security threat and risk assessments (TRAs) are conducted and risk mitigation activities established and assigned to responsible individuals. Data is backed up regularly.

We have procedures in place to detect, report and investigate data breaches. The company and its employees would be notified of any data breach as well as the Information Commissioner within 72 hours of us becoming aware of the breach.

A disaster Recover and business continuity plan have been developed and are tested and updated regularly.

We hold the ISO 27001 certificate for Information Security our certificate number is IS 711949 effective date 23rd March 2020. If you would like a copy of our certificate please contact the Operations Team.

14. **Hardcopy Documents Security.** We work electronically however there are occasions when data is in paper form. Any documents which give details of a company and its employees are disposed of using a confidential shredding service. All staff are trained to adhere to document usage procedures and must make sure that all paper documents which give details which would identify a company or a person are disposed of using the confidential shredding service. Staff are expressly prohibited from disposing of paper into waste paper bins or to take documents out of the office unless express permission is provided for example when visiting a company for a renewal meeting.
15. **E-mailing Sensitive Data.** There may be instances when we have to e-mail a document which holds personal or sensitive personal data to a third party as part of our brokering contract with them. In these instances we will encrypt the data being sent and use Transport Layer Security (TLS) with providers.
16. **Third Parties.** The personal data we hold about your employees is shared with third parties which will include insurance companies, cash plan providers and other companies who provide employee products. This is necessary for the performance of our role as independent intermediaries and the service we provide in arranging and administering insurance products.

## TERMS OF BUSINESS – CORPORATE - PAGE 4.

17. **advo on line and advo on line Plus.** In some instances, we will supply you and your employees with passwords to access our on line portal. This will give you and your employees the ability to view personal data, policy details, make amendments to personal data add and delete employees from products and services. The passwords issued are secure and generated automatically by our systems.
18. **Disclosure of Information.** It is important that you understand that any information, statements or answers made by you to us, or your insurer are your responsibility and must be correct. Any failure to disclose facts material to the insurer or any inaccuracies in your answers may invalidate your insurance cover in part or in whole. Facts material to the insurance are matters or information which may influence your insurer as to the acceptability or otherwise of your Proposal or Renewal and must be disclosed immediately. You are advised to keep copies of documentation sent to or received from us for your own protection.
19. **Awareness of Policy Terms.** When a Policy is issued you are strongly advised to read it carefully, as it is that document, the schedule and any certificate of insurance that is the basis of the insurance contract you have purchased. If you are in doubt over any of the policy terms and conditions please seek our advice promptly.
20. **Charges.** We will not charge you a fee for our services in connection with this policy. We are remunerated via commission from the insurance company providing your insurance or employee benefit. If you would like the details of the commission paid to us for your policy please let us know.

Fees. There may be occasion when we will charge a fee rather than commission. We will discuss this fully with you before any fees are accepted.

21. **Data Retention.** We are authorised and regulated by the Financial Conduct Authority. We have an obligation under this regulation to retain the records of your insurance and employee details for seven years. This is so that the regulator can verify that we have complied with our obligations with respect to our customers. We also have to retain records in the event of requests from customers who may require them for evidence when making a claim or if there is a complaint.

We are obliged to remove any individual who has the right to be forgotten and have processes in place to permanently remove an individual from our data base.

22. **Data Portability.** If requested we can provide individual client files in an excel spreadsheet format. This information will only include the information which was provided to us by the individual.
23. **Complaint handling.** It is our intention to provide you with a high level of customer service at all times. If there are occasions when we do not meet your standards please contact Mrs Gill Mateo either verbally or in writing, who will take details of your concerns. We will acknowledge in writing advising you of who is dealing with your concerns and attempt to address your concerns within five working days. If our investigations take longer we will provide a full response within twenty working days or explain our position and provide timescales for a full response. If we cannot satisfy your complaint you may be entitled to refer it to the Financial Ombudsman Service.

24. **Financial Services Compensation Scheme (FSCS).** We are covered by the FSCS. You may be entitled to compensation from the scheme if we cannot meet our obligations. This depends on the type of business and the circumstances of the claim. Insurance advising and arranging is covered for the first £2,000 and 90% of the remainder of the claim without any upper limit. Further information about the compensation scheme is available from the FSCS.
25. advo group follows data protection law.



A: advo group limited, advo house, St Leonards Road, Maidstone, Kent ME160LS  
T: 01622 769 210  
E: [Info@advogroup.co.uk](mailto:Info@advogroup.co.uk)  
W: [advogroup.co.uk](http://advogroup.co.uk)

Registered in England (No 4500663)