You have of rights of notification and control over your personal data which we store and process on our Company Secretarial System.

Under the General Data Protection Rules (GDPR) we hold data about you on certain vital computer systems, which enable us to provide an accurate and efficient service. In a complex, heavily scheduled and compliance laden world, modern accountancy practices would cease to function effectively without trusted software products.

We use a professional cloud based service called FirstOrder which enables us to interface electronically with Companies House to prepare and file documents like your annual Confirmation Statement. It also provides a repository for the statutory registers which your company is legally obliged to hold. By combining these and other filing requirements at Companies House and enabling the production of minutes etc to underpin the legality of your officer appointments and share transactions etc, this system enables us to provide accurate and timely filing and saves time and effort as well as enabling us to provide accurate and best value service.

Nearly all of the data we hold about you and your company on this system is already publicly available on the Companies House website.

However, some personal details are legally reportable but not publicly displayed by Companies House. If you or Companies House have provided them, the personal details we store on FirstOrder could include your residential address, date of birth, work phone, home phone, mobile, fax, DX number, DX Exchange and special three character identification "snippets" you may have volunteered if you have been involved with a company formation.

We use this data ONLY for the following

1) Ensuring you meet your statutory filing obligations at Companies House
2) Providing you with Minutes, Resolutions and Registers etc, which you have a legal obligation to create or maintain.

We have our own strict GDPR protocols so only trusted members of our staff are allowed to access or process your personal data.

Your personal data or statistics held on FirstOrder will NEVER be used for marketing or sales purposes.

No third party or any party other than those described above will ever receive any of your personal data or statistics, whether anonymously or identifiably.

Your personal data is only ever exchanged between FirstOrder and Companies House as the law requires.

Documentation produced by FirstOrder to enable us to meet your statutory requirements never leaves our office or archive facility, except to be transmitted to you.

We will only use your personal data in pursuit of providing our professional services to you.

You may receive automated requests for information from FirstOrder but solely in pursuit of providing our service to you and never for marketing or any other reason.

Your personal data is strongly encrypted on FirstOrder. Each individual has their own individual encryption key and your personal data is meaningless without this key which is separately generated. This offers data security far in excess of the basic GDPR requirement.

Your personal data is held on a dedicated single application in a secure server centre in the UK. Backups are also held offline in the UK. None of your data is hosted outside the UK.

You have a right to a copy of the details held about you on this system. To avoid any risk of impersonation, please contact us separately and identify yourself and we will send you a copy of the personal details we hold about you on FirstOrder. You also have a right to take your personal details to another provider and we can generate these for you in a portable format (.CSV). Please note that there is always a small risk in transmitting such personal data, normally held in encrypted form, through email or other electronic media when in human readable form.

You also have a "right to be forgotten" under GDPR. We will keep your personal details whilst you are a client. Government agencies may query your company or your role in it for up to seven years after you cease to be involved with it. For this reason we may keep your data in archive for this period before it is automatically deleted. Archived data is never accessed except on your request or that of Government agencies.

Please note that we would not keep your personal details on any computer system without very good reason and there are consequences in removing your details from FirstOrder. Your statutory registers would have to be kept by hand, minutes prepared by traditional word processing and your filing obligation met by using Companies House own website. We use carefully selected computer systems to improve efficiency and the inevitable consequence of being unable to do so would unfortunately impact us heavily and increase our costs. Other officers and shareholders in your company would be affected in the same way, as we cannot process companies unless we can process all the officers, members and shareholders involved. If you are involved with more than one company, this would apply to all your companies. As any alternative methods also carry their own data risks, we would ask you to consider the consequences very carefully before exercising this option and avoid doing so if at all possible.

We are primarily giving you this notification to meet compliance under the GDPR regulations. In practice, we have never had a data breach using this system and hope that the encryption information and reassurance given herein would be sufficient to enable us to continue using your details in a careful and professional manner on this very necessary software system.

General Data Protection Regulation (GDPR) – FirstOrder Secretarial

At First Corporate Law Services we are committed to data protection and GDPR compliance. We aim to answer the key questions regarding our measures to be GDPR compliant, so to provide complete assurance that your data is protected.

1. ***What are you doing/have you done to be GDPR-compliant?***

    a. Personal data will be encrypted on a field by field basis. Our clients will be provided with a compliance statement for onward distribution to their clients, outlining what data is encrypted under GDPR
    b. There will be a facility to export personal data as CSV upon client request
    c. There will be a facility to remove personal data upon request
    d. We will only process personal data where there is a lawful basis in doing so
    e. We will always seek, record and manage consent in line with GDPR compliance
    f. Our FCLS Group Ltd data protection policy is available on request

2. ***Where are your servers – inside or outside of the EU?***

Our servers are dedicated to our application alone and hosted in the UK in a fully managed secure server centre, by the UK's largest web hosting company.

3. ***What sort of physical and technical security protects your servers?***

Our backup is held on and offsite. The offsite backup is fully encrypted and managed by 'Xsystems Limited' on private UK based servers.

Our servers are fully equipped with firewall and suhosin server management software and all access attempts and targets are logged. The server and product have both been "black hat" tested by professional data security specialists.

4. ***Who has access to the servers and/or data?***

Our support staff (administrator users) will log in with two factor authentication (password and emailed key) and will be required to change their password weekly. Two developers have access to the server codes and rights to access data outside of the in-product authenticated user logins.

5. ***How often do your staff receive data protection training?***

All staff at FCLS Group Limited have received GDPR training and the measures that must be taken to comply with GDPR. Each individuals working practices have been reviewed and amended for compliance. An annual review will take place and further training provided as necessary. Each new staff member will receive training on GDPR.

6. ***Do you sub-contract your data processing to third parties? If so, how watertight are the third party's procedures and processes?***

Our servers are dedicated to our application alone and hosted in the UK in a fully managed secure server centre, by the UK's largest web hosting company.

7. ***Is access to your data user-based permission only?***

See point 3. Above.

8. ***How comprehensive are your back-up systems? (E.g. when was the last time/how often do they back up your data, and how far back can they go to retrieve it?)***

Our backup is held on and offsite. The offsite backup is fully encrypted and managed by 'Xsystems Limited' on private UK based servers.

Backups operate daily both onsite and offsite and a rolling 30 day backup of both is kept.

9. ***Have you ever experienced a data breach, or are there any perceived technical or operational weak links?***

There have been no breaches in the nine year life of the service.

In the event of a breach one of two things will happen according to the nature of the attack. If the server logs indicate no modification of the data (i.e. an attempt to corrupt the data) then the vulnerability will be traced in the source code or server set up as soon as possible and fixed. If the server logs show an attempt to corrupt the data, users will be notified and the data restored from the most recent un-affected backup. Simultaneously, the vulnerability is the server or source code will be addressed to prevent re-occurrence.