|  |  |  |  |
| --- | --- | --- | --- |
| **GDPR Self-Evaluation and Risk Assessment** | | |  |
| **Issue** | **Yes/No** | **Comments** | | |
| **Registration:** Are we registered with the Information Commissioner as a Data Controller? | **Yes** | The firm is to check that the renewal of the registration has been undertaken. | | |
| **Data Protection Officer (DPO):** Has the firm appointed a Data Protection Officer? | **No** | The firm is not required to appoint a statutory DPO under GDPR. However, it has decided to appoint a ‘Data Protection Manager’ in a voluntary capacity to lead on data protection and GDPR compliance. As the office manager, the post holder has the appropriate seniority to implement any changes necessary under GDPR. | | |
| **Cyber Essentials:** Is the firm accredited to the Cyber Essentials scheme? | **No** | The firm is not Cyber Essentials accredited, however, it believes that its Lexcel systems (after recently being updated for GDPR compliance) provide equivalent levels of security.  The officer manager is to review the situation and ask the Partners to make a final decision. The firm is undertaking a renewal of all hardware within the firm over the next few months and they believe that this will enhance the I.T security even further. | | |
| **Backup:** Is information appropriately backed up?  That includes electronic information being backed up offsite, and copies of important paper documents being made and kept separate from originals. | **Yes** | Backup arrangements are comprehensively set out in the Information Management and Security Policy (QPM Annex K). To reduce any loss suffered by the firm in the event of IT security breaches, the firm backs up all IT data on a regular basis to maximise business resilience. | | |
| **Retention:** Do we keep information for appropriate times?  Do we have clear time limits for the retention of records, in particular for matter files?  Do we safely dispose of confidential information when those time limits expire? For example:  - Are documents shredded rather than being placed intact in the refuse?  - Are electronic devices thoroughly cleaned of information before they are disposed of? | **Yes** | As set out in the Information Management and Security Policy (QPM Annex K), the firm maintains a detailed Information Asset Register setting out the personal data retained, its format, security, backup and retention arrangements.  Accounts records are maintained for at least six years as defined in QP12 of the QPM.  HR-related employee personal files are maintained during the course of employment and for a maximum 6 years after leaving  Payroll records are maintained for 6 years.  Recruitment records are kept for 12 months as set out in QP18 of the QPM. **The firm intends to review its procedures for retention and disposal of such documents to ensure that adequate controls are in place and documents aren’t held beyond the retention period.**  Client matter files are generally retained for six years with limited exceptions where longer periods are prescribed. These arrangements are set out in QP17 of QPM. The time periods are based on SRA/Law Society guidelines and have been subject to a risk assessment. Clients are notified of these storage arrangements in the firm’s T&C and closing letters.  Confidential papers are disposed of by specialist contractors as set out in Information Management and Security Policy (QPM Annex K) and Outsourced Services Policy (QPM Annex P). The contractors are required to sign a comprehensive confidentiality agreement. The contractors issue a certificate of destruction.  A rolling file destruction programme is in place (QPM QP17)  **The Principle of the firm recognise that a key challenge will be to develop processes for the destruction of electronic client/matter related documentation. Currently, a huge amount of historic client data is being kept that could and should be disposed of. A balance will need to be struck between the GDPR requirement to keep only what is necessary and the operational need of the firm to conduct conflict checks, for example. Further guidance from the Law Society will be sought.**  Cleansing of defunct electronic devices is set out in the Information Management and Security Policy (QPM Annex K). These will be wiped by the firm’s IT support consultants or the storage devices will be mechanically disabled by the firm. | | |
| **Security of Electronic Records:** Do we have effective safeguards against hacking, malware, phishing and other cybercrime? For example:  - Do we have a firewall to protect our intranet?  - Do we have up-to-date anti-virus software?  - Do we install software upgrades promptly?  - Do our systems have suitable password protection?  - Are passwords managed effectively? In particular do we ensure that passwords are of sufficient complexity and changed from time to time?  - Do our staff understand the risks and their responsibilities in respect of information security?  - Do staff understand the importance of reporting any breach of security?  - Do we circulate reminders about current risks and criminal methodologies? | **Yes** | As a Lexcel-based practice, these are Lexcel requirements and set out comprehensively in the Information Management and Security Policy (QPM Annex K).  The firm’s network has secure password management systems in place. User accounts are managed by the IT Manager. The firm’s systems are protected complex passwords which are subject to expiry periods.  Passwords are known only by staff members and are not written down. They are also changed on a regular basis to maintain privacy and the protection offered by a password.  Laptops and tablets are pass-coded. The laptops do permit access to the case management software and are all secure. Further checks will be undertaken by the firm.  **The firm is to look at options for encryption of laptops as a further precaution. In addition it will ensure that staff are given strict in instructions in the Lexcel procedures about not saving client/matter data onto portable devices to reduce the likelihood of breaches.**  The firm has procedures in place to deal with the email accounts of staff who have left the firm.  The firm’s general email traffic is not encrypted, however, some emails are encrypted emails via third party software such as Egress and CJSM.  Extensive data protection and security training is conducted at the firm to ensure all staff understand the risks and the need to report breaches. | | |
| **Security of Paper-Based Records:** Do we have appropriate security arrangements to protect paper-based records? For example:  - Are paper files well organised to minimise the risk of documents being lost?  - Is access to our premises appropriately controlled?  - Do we give staff clear guidelines about the risks involved in taking confidential papers out of the office, e.g. to court or to work on at home? | **Yes** | Procedures are set out comprehensively in the Information Management and Security Policy (QPM Annex K). Matter file organisation procedures are set out in QP09 of the QPM. Matter files are subject to regular reviews to ensure they are maintained in a tidy manner.  Physical security measures at the firm are robust and again set out in the Information Management and Security Policy (QPM Annex K).  Entry to the office is via the Reception Area which is policed by Reception staff thus preventing any unauthorised intrusion by clients or visitors. The Reception Areas are configured so as to prevent viewing of matter files and screens whilst in Reception.  Clear guidance to fee earners is given to fee earners (Annex F and Annex K) about protecting client confidentiality during client interviews. There are designated interview rooms at the firm’s premises which have no visible matter files in the rooms and hence no risk of confidentiality breaches. | | |
| **Collecting Personal Data:** Do we only collect and process personal data when we have a lawful basis for doing so? | **Yes** | This is set out in the Information Management and Security Policy (Annex K).  The firm regards Contract as the principal basis for collecting and processing client data. It also asserts that there is a ‘Legitimate Interest’ basis for limited marketing activity.  In the case of employees, the firm similarly regards Contract as being the lawful basis for processing employee data  The ‘consent’ legal basis within GDPR is only relied on in the event of any direct marketing activity to clients whereby opt-in client consent would be obtained. The firm currently has no plans for such marketing activity. | | |
| **Transparency:** Do we use appropriate privacy notices or other means where practicable to let people know the use we make of personal data we hold about them? | **Yes** | Set out in the Information Management and Security Policy (QPM Annex K). A Staff Privacy Policy is in place (QPM Annex W). The firm’s Terms and Conditions of Business set out privacy notices to clients. | | |
| **Training:** Overall, are staff adequately trained so that they understand their obligations under the GDPR and SRA Code of Conduct in respect of data protection, confidentiality, security and reporting of breaches? | **Yes** | Set out in the Information Management and Security Policy (QPM Annex K). Information management and security training is part of the firm’s Lexcel procedures. Training is also addressed in induction procedures with the Induction Checklist addressing GDPR and staff privacy.  **The firm has agreed to undertake data protection and security training to ensure all staff understand the risks and the need to report breaches. This will take place after the Lexcel systems are fully updated for GDPR and will be incorporated within a meeting.** | | |
| **Third Parties:** Have we considered the risks associated with us sending personal data and confidential information to third parties? This may include counsel, experts, accountants and consultants.  Is it adequate in all the circumstances for us to rely on the general data protection and confidentiality obligations of those third parties?  Otherwise, have we taken appropriate precautions? That may include the following.  - Checking that they have appropriate data protection procedures in place, including adequate security arrangements.  - Requiring them to agree to contractual terms. | **Yes** | Set out in the Information Management and Security Policy (QPM Annex K) and Outsourced Services Policy (QPM Annex P)  All outsourced services must sign a Lexcel-compliant confidentiality agreement. The firm has developed a Supplier Information Assurance Questionnaire which it is able to send to selected suppliers for when the firm requires additional assurance about a supplier’s GDPR protections. This will be subject to a risk assessment.  The firm currently regards none of its outsourced providers as presenting a high risk in terms of data protection. | | |
| **Marketing:** Do we ensure we do not send marketing communications without opt-in consent where that is necessary? | **No** | The firm’s marketing activity using client data is extremely limited and, in the unlikely event that it is undertaken, would be compliant under the ‘legitimate interest’ legal basis.  Any direct marketing activity undertaken in the future would only be directed at clients that have specifically opted in to marketing activity. This would be subject to a Data Protection Impact Assessment (DPIA) as set out in the Information Management and Security Policy (QPM Annex K) before commencing the activity. | | |
| **Automated decision making (including profiling):** Do we avoid using automated decision making about people?  Alternatively if we do use such techniques have we taken steps to ensure we comply with the particular obligations that apply? | **NA** | The firm has no automated decision making/profiling | | |
| **Subject Access Requests:** Are we adequately prepared to deal with any subject access requests we may receive from data subjects?  - Have we made it clear to staff to whom such requests should be forwarded?  - Are we able to retrieve documents or records sufficiently promptly?  - Do we have sufficient oversight over systems of the firm, so that relevant personal data can be searched without undue burdens? | **Yes** | Comprehensive procedures are set out in the Information Management and Security Policy (QPM Annex K). | | |

|  |
| --- |
| **Action points / additional comments** |
| The firm’s Lexcel QPM and associated documents including forms and terms and conditions of business were given an extensive update in July 2018 to comply with GDPR regulations. This has resulted in a number of significant changes both in the firm’s documentation and its practise. |

|  |  |
| --- | --- |
| **Signed (Data Protection Administrator)** |  |
| **Date** |  |