LOCKTON

Lockton Solicitors

GDPR SELF-ASSESSMENT CHECKLIST

Note: When completing this Checklist, an honest analysis is needed. So, for example, if you don't know the answer, just state "Don't know" or "Not sure". The purpose of this Checklist is to obtain an understanding of what steps need to be taken, if any, to achieve compliance with applicable data protection legislation. References in this checklist to Articles and Chapters, are to those contained in the UK GDPR.

QUESTION	RESPONSE
Data Protection Registration	
Is your registration up to date?	
Data Controller or Data Processor – Articles 4(7) and 4(8)	
Are you a data controller?	
Are you a data processor?	
Do you have any joint controller relationships?	
The Data You Hold	
Has your business undertaken a data mapping exercise to identify the personal data it holds (eg relating to staff, directors, shareholders, clients, suppliers, third party service providers)? Did the exercise flag any issues?	
Have you documented the following information required by Article 30(1) for records kept by data controllers and Article 30(2) for data processors): • The name and contact details of the data controller/joint controller/data processor and the data protection officer. • The categories of personal data you process (eg name, address, email address, passport, etc.). • Why you process it. • When it is processed. • Where it is processed (eg on internal systems, manually, electronic, on phones, laptops, off-site, held on cloud, etc). • Where you obtained it from. • Who you share it with (if anyone) • When you transfer data outside your organisation. • Any technical and organisational security measures (Article 32(1)).	

Lawful Basis for Processing Data - Article 6	
Have you established one of the six lawful bases for processing your personal data and documented this in your records? (Note: the commonly used bases are set out below with further questions)	
Consent – Articles 6(a) and 7	
If you rely on consent as the basis for processing, have you considered how you collect this and whether you record consent when obtained?	
Do you have/have you established a method or system for recording consent?	
Have you informed data subjects that they can withdraw consent? If so, how can they do this and how do you record it?	
Contract – Article 6(b)	
Is your processing necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract?	
Legal Obligation – Article 6(c)	
Is the processing necessary for you to comply with the law (not including contractual obligations)?	
Legitimate Interest – Article 6(f)	
Is the processing necessary for your legitimate interests or the legitimate interests of a third party, (unless there is a good reason to protect the individual's personal data which overrides those legitimate interests?	
Sensitive Data – Article 9 **Note:** you may hold this type of information in your employment records. **Note:** To lawfully process special category data, you must identify (i) a lawful basis under Article 6 and (ii) a separate condition for processing special categories of data under Article 9 (these don't need to be linked).	
Do you collect any sensitive data (eg information relating to health, race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), sex life or sexual orientation)?	
Have you identified your lawful bases for processing this type of data?	
Have you introduced any special measures or controls when processing this type of data?	

CCTV
Do you use CCTV?
If so, do you notify data subjects that CCTV is in use by using a clear notice or other method?
Is the footage made public or shared with third parties?
If so, for what reason?
Is there a process in place for obtaining consent of processing this data? (Article 9)
Is there a process in place for data subjects to obtain footage? Either video or audio. (Art 15)
Is there a process in place for erasing data of this nature? (Art 17)
Transparency – Articles 13 and 14 set out what you must tell individuals
Do you notify data subjects that you are processing their data (eg through your privacy policy)?
Is data always collected direct from data subjects or do you ever obtain it from third parties?
When you collect data, do you give data subjects the information required under data protection legislation at the point of collection (eg through your privacy policy)?
Data Protection Officer – Article 37
Do you have a Data Protection Officer?
If so, have you published the contact details of the Data Protection Officer and communicated this to the ICO?
If not, who is responsible for data protection at your firm?
What is their job title?
Have you considered whether you need to appoint a Data Protection Officer for the purposes of UK GDPR?
Accountability – Article 5(2)
How often is data protection and compliance with GDPR/ Data protection legislation discussed at management/ governing body level?
Has the management/governing body appointed a specific director/partner/member to have responsibility for all data protection matters?
Does the person responsible for data protection have direct access to the management/governing body?

Data Protection Policies and Procedures – Article 5(2)
Do you have policies and procedures in place dealing with data protection generally, including information security management?
Do the policies and procedures cover the seven key Data Protection principles: • Lawfulness, fairness and transparency • Purpose limitation • Data minimisation • Accuracy • Storage limitation • Integrity and confidentiality (security) • Accountability
Lawfulness, fairness and transparency. This means:
• You need to identify your lawful basis for collecting and using personal data. • You ensure you don't do anything with data in breach of any other laws. • You must use personal data in a way that is fair (i.e. not process it in a way that's unduly detrimental, unexpected or misleading to the individuals concerned). • You are clear, open and honest with people from the start about how you will use their personal data.
Data minimisation. This means:
You only collect what's necessary for the purposes for which it's collected.
Accuracy
You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact. How do you ensure that personal data is kept up to date and accurate?
Storage limitation (retention)
You must not keep personal data for longer than you need it. Does your privacy policy include information on retention of data? Do you have policies and procedures in place for archiving and destruction of data?

Integrity & Confidentiality (the 'security' principle)
You must ensure that you have appropriate security measures in place to protect the personal data you hold. Are appropriate security measures used to protect the data?
Are your systems subject to regular penetration testing?
Accountability
You take responsibility for what you do with personal data and how you comply with the other principles. You have appropriate measures and records in place to be able to demonstrate your compliance. Is your management/governing body fully aware of their data protection obligations as regards the principle of Accountability?
Has the management/governing body ever received training on data protection?
Is the management/governing body able to demonstrate how it discharges its obligations under data protection law?
Data Subject Rights – Chapter III
Access to Personal Data
Have you ever received a subject access request (SAR)?
Have you put documented policies and procedures in place for handling SARs?
Are you confident that you will be able to respond to requests within one month as required by law?
How do you inform individuals how to request the information you hold about them (this is generally via your privacy policy)?
Have staff received training on how to identify a subject access request (as these can be received in a number of ways including by telephone, via social media, in writing, in person)?

Privacy Policy	
Does your privacy policy include all of the information required by Article 13 including (this list is not exhaustive): • The identity and the contact details of the controller. • The contact details of the data protection officer, where applicable. • The purposes of the processing for which the personal data are intended as well as the legal basis for the processing. • Where the processing is based on the transfer of data internationally, the legitimate interests pursued by the controller or the third party. • The recipients or categories of recipients of the personal data, if any. • The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. • The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability. • The right to lodge a complaint with a supervisory authority. • Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data. • For any other purpose the reason for doing so.	
Profiling and Automated Processing (Article 13(2)(f) & Article 22(1) and (4)	
Do you undertake any profiling (under data protection law automated processing of data to analyse or to make predictions about individuals)?	
If so, do you have explicit consent?	
Data Portability	
If requested, can individuals obtain their personal data in a structured, commonly used and machine-readable format if requested? (Note: This right allows individuals to obtain and reuse their personal data for their own purposes across different services and only applies where you are carrying out the processing by automated means).	

Data Security – Article 5(1)(f)	
Appropriate Technical and Organisational Measures	
Have you reviewed the risks inherent in processing personal data at your firm?	
What steps did you take to mitigate any risks?	
Do you have an Information Management Security policy in place that specifies the safeguards you have in place?	
Do you have an Internet Use policy in place?	
Do any staff access systems from home via laptops or mobile devices?	
If so, do you have a Working at Home policy?	
How do you hold personal data at your firm?	
Is it encrypted or anonymised or destroyed when no longer needed?	
Do you pseudonymise or anonymise any personal data? **Note:** Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual. It does not change the status of the data as personal data. Recital 26 of UK GDPR makes it clear that pseudonymised personal data remains personal data and within the scope of the UK GDPR. Note: UK GDPR does not apply to personal data that has been anonymised. To be properly anonymised under UK GDPR, you must strip personal data of sufficient elements that mean the individual can no longer be identified. But, if you could at any point use any reasonably available means to re-identify the individuals to which the data refers, that data will not have been effectively anonymised but will have merely been pseudonymised.	
Have you considered the security of data for staff who may be working at home?	
What security measures have you put in place?	
Data Breaches	
Do you have formal mechanisms (ie policies and procedures) in place to identify data breaches and how to handle incidents?	
Are the mechanisms subject to monitoring and review and have they been tested?	
Do you have procedures in place to ensure your Privacy Officer (or equivalent) and data subjects (where required under data protection law) are notified of data breaches?	
Do you have internal guidance explaining to staff when notification is needed and what and how they need to report? (Note: All breaches should be reported, eg sending emails or post to wrong addresses).	
How do you inform staff of reporting?	

Data Breaches
Have you considered data breach insurance cover?
Do you have a data breach register?
Using Others to Process Your Data
Do you use anyone else to process personal data (eg payroll providers, pension administrator)?
Have you reviewed and updated any contracts you have with third party processors: (i) so that they contain the provisions required under data protection law (see Article 28(3)) and (ii) to indemnify you against any loss you suffer as a result of breaches?
Do you employ contractors/ consultants and if so, do they handle personal data on your behalf?
Do your contracts with them include data protection provisions where necessary?
Do you undertake due diligence on third party providers to check their information security procedures?
International Data Transfers – Chapter V
Is any personal data transferred outside the UK?
If so, what type of personal data is transferred and to whom?
Do you know if transfers are compliant with data protection law (eg are they either covered by an adequacy decision, or covered by an exception)?
Do you or any sub-processor hold any of the firm's personal data in a cloud? If so, do you disclose this in your privacy policy?
If so, do you disclose this in your privacy policy?
Marketing
Do you undertake any form of marketing or promotion to clients?
If so, how have you obtained consent to market and did you provide an opt-out to marketing at the point of data collection?
Do you collect data when people visit your firm's website?
If so, is your firm's Privacy Policy clearly displayed on your website?
Is your Privacy Policy referred to in your terms of business?

Data Protection Impact Assessments	
How often do you implement or consider new projects where personal data may be used?	
Do you undertake a Data Protection Risk/Privacy Impact Assessment when necessary (when processing is likely to result in a high risk to the rights and freedoms of individuals)?	
Are projects reviewed during development, testing and delivery stage, ie pre- and post-implementation?	
General	
When was your Privacy Policy last updated?	
How do you provide this to clients? Is it referred to in your client care letter or terms of business?	
Did you provide a copy of your updated Privacy Policy to existing clients/staff when updated to comply with data protection changes in 2018? If so, how was this done?	
Has your HR function reviewed its contracts and Staff Handbook so that they comply with data protection law?	
How do you provide employees with privacy information (this is generally via a link to a privacy notice and may be found in your Staff Handbook or referred to in your contracts of employment)?	