pitmans law

GDPR 5x5 risk assessment checklist

This checklist takes you through the questions you need to be answering to identify areas of risk in your information security regime.

As a business we're using this checklist to address our own compliance with GDPR and we're working through it with our GDPR clients to provide process guidance to mitigate risk.

1 DATA PROTECTION ARRANGEMENTS – Do you have the following arrangements in place?

1. A general data privacy policy and (as part of that or separately) an information security policy?
2. A designated individual responsible for data privacy and information security?
3. A programme of regular reviews to assess risks in your arrangements and monitor the effectiveness of mitigation strategies?
4. Up to date record keeping in relation to risk assessments and risk mitigation?
5. A programme of regular training and education for staff and external contractors who deal with data?

2 DATA STORAGE – Thinking about the location of data you control do you...

1. Have and maintain an up to date data map of the different locations within which personal data is processed?
2. Undertake regular checks of the integrity of that data?
3. Only store data on encrypted storage devices?
4. Have in place adequate technological measures to prevent unauthorised access to the data, including security arrangements?
5. Have policies about how, when and why data may be accessed and who by, and have mechanisms to secure compliance?

3 DATA ACCESS – Under what circumstances is data ever processed outside of your systems?

1. Do staff work remotely? If so, do they access data in a structured way over a secure connection?
2. Is there a policy in place restricting staff from exporting data and do you monitor compliance?
3. Where third party organisations process data on your behalf are they subject to strict contractual terms in line with your internal policies?
4. Do you take adequate measures to ensure that third party data processors have adequate systems and safeguards in place?
5. Are your processes and these measures properly documented and auditable?

4 DATA BREACHES – In the event of a data breach...

1. Do you have systems and policies in place to ensure that any breach is identified promptly and reported?
2. Do you have a process for gathering the information required to assess whether a breach notification is required?
3. Is there someone designated as responsible for making breach notifications and has cover been arranged in their absense?
4. If data is lost or corrupted, do you know how much of it will be able to be restored or checked against backups?
5. Do your policies extend to identification and mitigation of risks which are identified without any data being compromised?

5 MAINTAINING DATA – Retention/disposal of data

1. Do you have policies and processes in place to ensure that data is only retained for as long as it is necessary and lawful to do so?
2. Are there automated systems in place to monitor and identify any data which has been retained outside of those policies across all of the digital estate within which data might be located?
3. Is there a process for the secure disposal of data after its retention is no longer appropriate?
4. Are these arrangements properly documented and auditable?
5. Do you ensure that equivalent measures are in place with any third party data processor or on staff's own devices (if you have a Bring Your Own Device policy)?

About Pitmans Law Data Protection

It is increasingly important for businesses to embed privacy, by design and by default, into every aspect of your activities.

Our approach is to build a deep understanding of the specifics of your business so we can identify your data protection issues throughout the duration of your customer and employee relationships as well as the lifecycle of your company.

Our comprehensive services include:

Process: legal advice around process improvements for established businesses

Documentation review: to ensure existing privacy statements and contracts are compliant with current and future legislation

Breaches: breach notification to the ICO, navigating fallout with stakeholders, dealing with threatened claims and litigation against providers in your supply chain

International: assisting international clients to understand their obligations when they are processing the data of EU citizens

Start ups: advisory work to ensure that the complex legislative regime around data protection is adhered to from the ground up

pitmans law

We act for a diverse range of domestic and international clients, from start-ups to multinationals, and everything from tech companies leveraging big data in their service offerings through to charities navigating a response to a subject access request for the first time.

"The level of service has always been exemplary; they are fast to respond, proactive in approach and have a deep understanding of our business due to a long-term relationship."

Contact me for more information

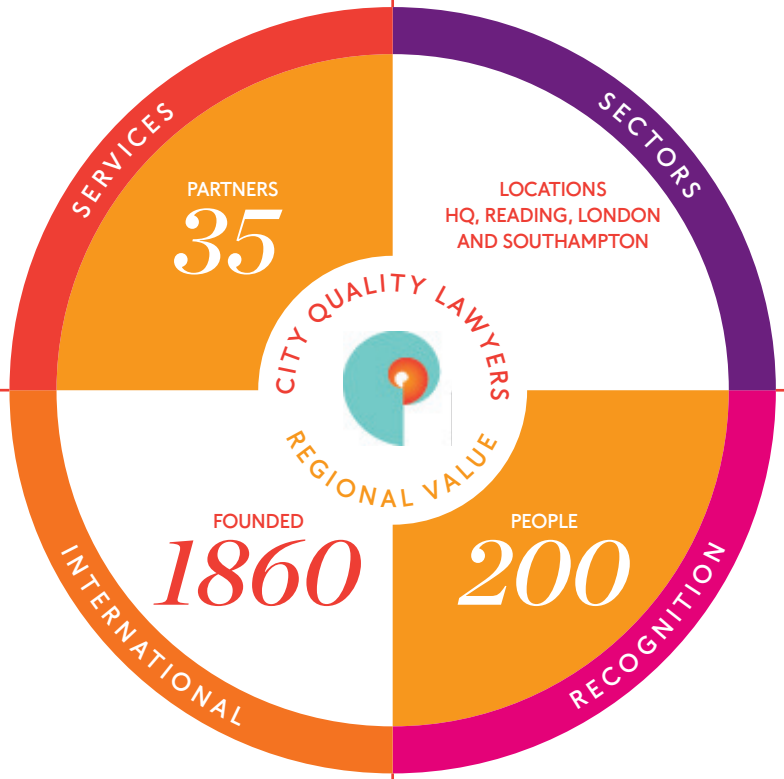
Will Richmond-Coggan
Data privacy Partner
D 0118 957 0369
M 0788 181 4302
E wrcoggan@pitmans.com

About Pitmans Law

Banking & Finance
Commercial
Corporate
Data Protection
Debt Recovery
Dispute Resolution
Employment
Insurance
Intellectual Property

Matrimonial & Family
Pensions
Real Estate
Restructuring & Insolvency
Wills, Tax & Trusts

14
Areas of expertise



Banking
Charities & Not for Profit
Energy
Hospitality
Insurance
Life Sciences
Real Estate
Retail
TMT
Transport

10
Sector specialisms

Over **25**
firms worldwide

The founding UK member firm of the global legal network, Interact Law

21 Individuals **"Recommended"** by Chambers

25 Practice areas "Ranked Highly" by legal 500

Tier 1 Ranked
Top 150 Law Firm
Regional Heavyweight
Lawyer 200 Star Performer

Award winners

Lawyer of the year
Law Firm of the Year
Lex 100 Best Work/ Life Balance

pitmans law

With Pitmans Law you can be assured of the quality of advice and service you demand from a city law firm – but with a distinction. The courage to stand apart, to think and act personably, with an uncompromising focus on achieving outstanding client outcomes. We say what we mean, matching our behaviours to our words.

Established for over 150 years, Pitmans Law is headquartered in Reading with offices in London and Southampton. The lower overheads of a regional office ensure we can provide city quality legal advice at a competitive price to deliver exceptional value for our corporate and private clients locally, nationally and internationally.

Pitmans provides legal advice to address our clients' needs across a wide range of industry sectors and specialisms including particularly strong specialist teams in pensions advisory, real estate, dispute resolution as well as corporate and commercial law. Our clients draw confidence from the top tier recognition Pitmans achieves in the industry benchmarking directories, Legal 500 and Chambers UK.

Contact us
T +44 (0)345 222 9222
E law@pitmans.com