GO2 Consulting Services Ltd
Your reliable, trusted and confidential adviser

GDPR - 5x5 Risk Assessment Checklist

It's never too late to improve

	☐	**DATA PROTECTION ARRANGEMENTS – Do you have the following arrangements in place?**
1	☐	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?
	☐	**DATA STORAGE – Thinking about the location of data you control do you...**
2	☐	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?
	☐	**DATA ACCESS – Under what circumstances is data ever processed outside of your systems?**
3	☐	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?
	☐	**DATA BREACHES – In the event of a data breach...**
4	☐	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 absence?
	☐	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?
	☐	**MAINTAINING DATA – Retention/disposal of data**
5	☐	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)?