GDPR CHECKLIST FOR FUNDS

GDPR came into force in May 2018. Here's a summary of what investment funds businesses need to consider and action to comply with GDPR.

	STEPS	GDPR PRINCIPLE
1.	**Confirm applicability and audit data flows** - Identify legal entities to which GDPR applies, both in the EEA and outside. - Determine what data is being handled, between which entities/service providers and in what capacity (controller or processor?)	*Lawfulness, fairness & transparency*
2.	**Check and confirm legal basis for processing** - Identify where consent is relied on to process personal information, identify the flow of investor personal data to and between fund parties, and determine the legal basis for lawful processing. Reflect legal basis in updated notices. - Update and publish revised consent wording. - Develop process to track consents, non-consents and withdrawal of consents. - Ensure adequate protections are in place and that consent is sought for sensitive personal information.	*Lawfulness, fairness & transparency* *Data minimisation*
3.	**Comply with notice obligations** - Publish GDPR-compliant privacy notices (employee and investor). - Consider the need for enhanced notices in prospectuses and subscription documents.	*Lawfulness, fairness & transparency*
4.	**Put procedures in place to safeguard data subjects' rights** - Draft procedures to receive and respond to access, correction and data portability requests, and to restriction-of-use requests and objections. - Implement and embed these procedures into existing processes and determine if investor consent is required.	*Accurate and up to date* *Accountability & record keeping*
5.	**Ensure accountability and data protection by design/default** - Review, update and implement data protection policies, codes of conduct and related procedures, training materials and any additional policies required. Monitor and audit compliance with all such policies. - Add privacy and data security to review processes for new services and implement training on the same. - Review and address DPIA requirement.	*Accountability & record keeping* *Limit on data retention*
6.	**Ensure appropriate data transfer mechanisms are in place**	*Data security*
7.	**Review and address service provider contract requirements** - Update existing service provider/data processor templates, and review and update existing key contracts.	*Data security*
8.	**Review and address security breach notification requirements** - Revise incident response plans to allow for 72-hour timeframe and consider whether amends need to be made to contractual agreements with service providers. - Provide training on the revised response plans.	*Data security*
9.	**Determine whether to appoint a Data Protection Officer**	*Accountability & record keeping*