DUE DILIGENCE DOCUMENT

Provider/Supplier Due Diligence Document/GDPR

CONTRACT	
Does the agency agreement define our mutual responsibilities under GDPR?	Yes
Does it make it clear the Providers/Suppliers responsibilities in the case of a breach?	Yes
Have Grove updated our own employment contracts to define GDPR responsibilities?	Yes

SYSTEM SECURITY	
Does Grove take responsibility for the security of our data internally or do we outsource to a Third Party?	Yes, internally.
Does Grove conduct regular security testing?	Business Continuity and Disaster Recovery Tests are carried out on a routine basis.
Have reasonable steps been taken to protect our systems?	Yes, we implement an Onion layer approach to our security systems, utilising various platforms. Physically building is alarmed, Comms room locked, comms cabinet locked and monitored via CCTV throughout.
Is data encrypted 'at rest' and 'in flight' including data exchanges Application Programming Interfaces (APi's))?	Our CRM is encrypted at rest and uses either SSL or TLS encryption in transit. Additionally, access to that data is whitelisted to single authorised IP.
Does Grove have information security and data protection policies?	Yes, within our IT Infrastructure and Security Framework Declaration along with our BCP.

Grove Pension Solutions Ltd – Registered in England – Company number 06045836
New Grove House, Murray Road, Orpington, Kent, BR5 3QY - 01959 534 082 - info@groveps.co.uk - www.grove-pensions.co.uk
Authorised and regulated by the Financial Conduct Authority. Reference number: 465051

DATA SUBJECTS

Does anyone outside of the Grove organisation have access to data subjects and our client data?	Yes, this is carefully reviewed, and access provided strict criteria has been met.
What data can they see and for what reason?	Data we allow the vendor in question to access – maintenance of database and ancillary software, all covered by Processor Agreements.
Does Grove use 'privacy by Design' as a principle?	Yes, as part of GDPR compliance, we have undertaken Data Processing Impact Assessments to ensure complete data privacy and security.
What access rights does Grove give to data subjects?	As per GDPR. This is written into client agreements.
Are appropriate confidentiality / NDA agreements in place including with any third parties that are involved in the provision of services.	Yes, confidentiality integrated into signed staff contracts. Privacy statements in place for all third parties.

DATA SECURITY

Can Grove fulfil a subject access request?	Yes
Can Grove log changes to data and report on these changes?	Yes
Is Grove able to log and implement right to be forgotten requests (RTBF)?	Yes
Can Grove provide data portability in a usable format?	Yes
Does Grove store paper files and removable IT media in lockable filing cabinets?	Yes, all staff have lockable filing cabinets and adhere to a clear desk policy.
How does Grove dispose of confidential waste (e.g. secure shredding on or off-site)?	Secure shredding onsite.
How is electronic media disposed of? Is data deleted or continuously overridden, a technique known as "electronic shredding"? Or are data media physically destroyed?	We no longer utilise electronic media for data storage purposes. Data is backed up utilising 448 Bit military encryption to a secure cloud vendor.

Does Grove have a Network Firewall and Policy, Web / Email Filtering Policy and tools, Anti-malware solutions, O/S, network and application patching policies?	Yes, covered within our IT Infrastructure and Security Framework declaration.

INSURANCE

Does Grove carry professional indemnity insurance? Details.	Yes, £1,700,000 any one claim and in the aggregate. Excess £20,000.

FINANCIAL STABILITY

Is Grove financially sound?	Yes, meet FCA Financial Resources Requirement.
Has Grove ever taken out a loan?	No, never.

PRIVACY BY DESIGN

Does Grove restrict data access to only authorised personnel?	Yes
Does Grove encrypt data (i.e. passwords)?	Yes, data is encrypted on and password hashes utilised rather than the password itself. Email encryption services are used for protecting sensitive or confidential information in transit. Remote workers access to company resources via use of a corporate VPN with multifactor authentication.
Does Grove use open source platforms, such as WordPress?	Yes, on website but any client data is encrypted.
If yes, has Grove undertaken a GDPR DD exercise on our own 3rd party providers?	Yes

DATA RECOVERY

What is Grove's data backup policy in the event of a system failure?	Daily backups performed. RTO &RPO listed. Restore accomplished via cloud back up system (off site) or near line back up system (secure-on site).
Does Grove have a Business Continuity Plan?	Yes, comprehensive Business Continuity Policy ensures quick access to data and services through cloud backups and other technologies. Recovery Time Objective: 4 hours Recovery Process Objective: 7 hours
Does Grove have a clearly defined data recovery policy, which includes protocols to ensure there is no breach when restoring data?	Yes, included as part of the BCP.

DATA BREACH

Does Grove have a clean recording pathway in the event of a breach?	Yes, process and training in place.
Does this process include a procedure for how Grove will inform the Data Subject?	Yes
Does this process include a procedure for how the Provider/Supplier will inform any relevant Third Parties?	Yes
Does Grove have appropriate mechanisms for monitoring system activities and highlighting potential breaches?	Yes, auditing and Compliance software installed.

OPERATIONAL RISK AND COMPLIANCE

FCA registration firm reference number	465051
Can Grove confirm that we are GDPR compliant?	Yes

Has Grove been investigated by the FCA either previously or currently or have any known pending investigations	Yes, we have had a number of routine interactions with the FCA over the years, including most recently being part of their supervisory assessment into DB pension transfers. This covered every aspect of how our business operates along with file reviews. There are not any issues.
A brief overview of the experience/qualifications of the PTS's at Grove	We have 2 fully qualified PTS's, both with over 20 years industry experience and 9 and 5 years respectively, working at Grove, dealing with nothing else other than pension transfers.
Does Grove have adequate structures in place to ensure that areas of emerging risk are identified, managed and escalated in a timely and appropriate manner?	Yes, at senior management weekly meetings (documented).
Does Grove have an adequate framework in place to prevent / minimise fraudulent activity among our employees, workers and third parties?	Yes, employees are trained in Financial Crime prevention. Senior staff and advisers are regularly credit checked. Advisers are not paid on a commission basis. Third parties have privacy policies and /or signed contracts. All financial organisations with whom we do business are all checked for FCA registration.
Does Grove have a policy in place to ensure compliance with Anti-Bribery / Corruption legislation	Yes, policy and training in place.
Does Grove apply a recruitment, vetting and verification process for personnel who are performing services under the contract?	Yes, ID checks for all staff. Scanned copies of original, relevant qualifications etc. for advisers and paraplanners where relevant. Regular credit checks for senior managers and advisers.