PKBCIVILS

GDPR Statement

In our capacity as Data Processor, we will perform our obligations only in line with documented instructions from the Client and in accordance with applicable laws such as GDPR, PECR and ICO guidelines.

- We will not process the Data for our own purposes or those of any third party.
- We will not transfer the Data (nor permit the Data to be transferred) outside of the European Economic Area ("EEA") unless the Customer gives us prior written consent/ instruction to do so, in which case we will take the necessary measures to ensure that the transfer is in compliance with applicable Data Protection Law.
- We will ensure that any person whom we authorise to process the Data (including our staff, agents and subcontractors) will be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and we will not permit any person to process the Data who is not under such a duty of confidentiality.
- We will implement the appropriate technical and organisational measures to protect the Data from loss, alteration, unauthorised disclosure, or access to the Data, whether accidental or malicious in nature.
- We may from time to time subcontract processing of the Data to a third party subcontractor without the specific written consent of the Customer, in cases such as repairs to data centres, switching of certain service providers (e.g. hardware providers, software providers or providers of other services related to Cloud Computing) as these instances would be classed as being in the legitimate interest of the Data Controller (Recital 49 of the GDPR) and other exemptions made by the ICO for cloud providers. We reserve the right to sub-contract vetted tech specialists for the occasional or regular provision of certain cloud-related services. Your acceptance of this Scope Document implies your awareness and consent in this regard.
- Our GDPR Terms reflect the commitments required of processors in Article 28.

Article 28 requires that processors commit to:

- Only use sub processors with the consent of the controller and remain liable for sub processors.
- Process personal data only on instructions from the controller, including regarding transfers.
- Ensure that persons who process personal data are committed to confidentiality.
- Implement appropriate technical and organizational measures to ensure a level of personal data security appropriate to the risk.
- Assist controllers in their obligations to respond to data subjects' requests to exercise their GDPR rights.

- Meet the breach notification, rectification and assistance requirements set out in Article 28
- Assist controllers with data protection impact assessments and consultation with supervisory authorities.
- Delete or return personal data at the end of provision of services.
- Support the controller with evidence of compliance with the GDPR

In the event of a security breach involving, PKB would liaise with the relevant customer contact(s) notifying them of the nature of the breach, impact and other details and communicate progress throughout, according to agreed reporting channels.

A security incident would be raised, and an investigation commenced to identify what immediate action is necessary to contain the breach, what longer-term preventive action is required, identify root cause and conduct required corrective actions.

Actions are monitored for effectiveness through to resolution. All incidents are categorised to identify any trends/patterns which may require a focused initiative to address.