DATA PROCESSING AGREEMENT

AGREEMENT DATED DATE

BETWEEN:

FIRM NAME

and

REP NAME

BACKGROUND

1. This Agreement is to ensure there is in place proper arrangements relating to personal data passed between the Data Controller and the Data Processor;

2. This Agreement is compliant with the requirements of Article 28 of the General Data Protection Regulation;

3. The parties wish to record their commitments under this Agreement;

IT IS AGREED AS FOLLOWS:

4. DEFINITIONS AND INTERPRETATION

In this Agreement:

5. "Data Protection Laws" means the Data Protection Act 1998, together with successor legislation incorporating GDPR;

6. "Data" means personal data passed under this Agreement, being in particular any information about detainees or provided by detainees held in custody by the police who

require or request legal advice, including police disclosure, client instructions and legal advice provided to the defendant or detainee along with any other information obtained in the ordinary course of our business;

7. “GDPR” means the General Data Protection Regulation;

8. "Services" means giving legal advice to defendants in police custody who are to be interviewed under caution along with any other service provided by the Processor in the ordinary course of its business;

9. “The Controller” is FIRM NAME the Data Controller;

10. “The Processor” is REP NAME who is the Data Processor;

SUMMARY

11. All mobile devices, computers, servers and other digital devices used by the Processor and the Controller are at a minimum password protected and preferably encrypted;

12. Materials arising from police station attendances are kept secure at all times and are kept in the Processor’s and the Processors representative’s and nominees immediate personal possession at all times without exception;

13. Materials arising from police station attendances are handed in to the Controller within 24 hours of the attendance;

14. Any files are removed from the Controller's offices only with express prior permission;

15. Files and information relating to clients are never disclosed to others including experts and barristers without express prior permission of the Controller;

16. The Processor if aware of any data loss event will report immediately to the Controller;

17. The Controller if aware of any data loss event will report immediately to the Processor;

DATA SECURITY

18. The Processor and the Controller will ensure that the data transferred between them is kept confidential and is stored and processed securely and in any event in accordance with the requirements of the General Data Protection Regulation (GDPR);

19. If any data is in paper format the Processor and the Controller will keep files and information in a secure and locked environment, transporting files and information securely, and not leaving files or information unattended

in places where they are at risk (such as in cars, conference rooms or other public places);

20. The Processor and the Controller will use data for no purpose other than the purpose for which it was provided;

21. The Processor and the Controller will keep records of any processing activities;

22. The Processor and the Controller will ensure that in the event of either organisation requiring a mandatory Data Protection Officer such a person is appointed and registered with the ICO;

23. Otherwise the Processor and the Controller will ensure there is a person identified within the organisation to ensure that all GDPR requirements are met and to lead on all data issues;

24. The Processor and the Controller will ensure that anyone processing the data is subject to a duty of confidence (i.e. that they and their staff have signed confidentiality agreements);

25. The Processor and the Controller will assist each other in providing subject access and allowing data subjects to exercise their rights under the GDPR;

26. The Processor and the Controller will assist each other in meeting GDPR obligations in relation to the security of processing, the notification of personal data breaches

and data protection impact assessments and notify each other immediately if any breaches occur whilst you are processing the data;

27. The Processor will delete or return all personal data as requested to the Controller at the end of each case;

28. The Processor and the Controller will submit to any audits and inspections, and provide any evidence which may be required to assess suitability as a data processor or data controller;

29. The Processor and the Controller will cooperate with the relevant Data Protection Authorities in the event of an enquiry;

30. The Processor and the Controller will provide whatever information is needed to ensure they are are meeting their obligations;

31. The Processor and the Controller will immediately inform each other if either are asked to do something infringing the GDPR or other data protection law;

AUDITING

The Controller is audited by various third parties, including the Information Commissioner, the Legal Aid Agency, the Solicitors Regulatory Authority and a quality mark

assessment body. The Processor will give them every cooperation;

DATA PROCESSING

32. The Controller is the data controller for the Data and the Processor is the data processor for the Data. The Data Processor agrees to process the Data only in accordance with Data Protection Laws and in particular on the following conditions:

33. The Processor shall only process the Data:

(i) on the written instructions from the Controller;

(ii) only process the Data for completing the Services and

(iii) only process the Data in the UK with no transfer of the Data outside of the UK (Article 28, para 3(a) GDPR);

34. Ensure that all employees and other representatives accessing the Data are:

(i) aware of the terms of this Agreement and

(ii) have received comprehensive training on Data Protection Laws and related good practice, and

(iii) are bound by a commitment of confidentiality (Article 28, para 3(b) GDPR);

35. The Controller and the Processor have agreed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, complying with Article 32 of GDPR, details of those measures are set out under Part A of the Annex to this Agreement (Article 28, para 3(c) GDPR);

36. The Processor may involve any third party in the processing of the Data without the consent of the Controller. Consent may be withheld with reason. Consent is given without a further processing agreement (Article 28, para 3(d) GDPR). The Processor is an agent and provides supervised and qualified police station representation to the Controller's clients;

37. Taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, in so far as this is possible, for the fulfilment of the Controller's obligation to respond to requests from individuals exercising their rights laid down in Chapter III of GDPR – rights to erasure, rectification, access, restriction, portability, object and right not to be subject to automated decision making etc (Article 28, para 3(e) GDPR);

38. Assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of GDPR – security, notification of data breaches, communication of data breaches to individuals, data protection impact

assessments and when necessary consultation with the ICO etc, taking into account the nature of processing and the information available to the Processor (Article 28, para 3(f) GDPR);

39. At the Controller's choice safely delete or return the Data at any time. [It has been agreed that the Processor will in any event securely delete the Data at the end of the Services]. Where the Processor is to delete the Data, deletion shall include destruction of all existing copies unless otherwise a legal requirement to retain the Data. Where there is a legal requirement the Processor will prior to entering into this Agreement confirm such an obligation in writing to the Controller. Upon request by the Processor shall provide certification of destruction of all Data (Article 28, para 3(g) GDPR);

40. Make immediately available to the Controller all information necessary to demonstrate compliance with the obligations laid down under this Agreement and allow for and contribute to any audits, inspections or other verification exercises required by the Controller from time to time (Article 28, para 3(h) GDPR);

41. Arrangements relating to the secure transfer of the Data from the Controller to the Processor and the safe keeping of the Data by the Processor are detailed under Part A of the Annex;

42. Maintain the integrity of the Data, without alteration, ensuring that the Data can be separated from any other information created; and

43. Immediately contact the Controller if there is any personal data breach or incident where the Data may have been compromised;

Termination

44. The Controller may immediately terminate this Agreement on written notice to the Processor;

45. The Processor may immediately terminate this Agreement on written notice to the Controller;

General

46. This Agreement may only be varied with the written consent of both parties;

47. For the purposes of this Agreement the representatives of each party are detailed under Part B of the Annex;

48. This Agreement represents the entire understanding of the parties relating to necessary legal protections arising out of their data controller/processor relationship under Data Protection Laws;

49. This Agreement is subject to English law and the exclusive jurisdiction of the English Courts;

Signed For and on behalf of FIRM NAME

……

Name:

DATE

Signed For and on behalf of REP NAME

……

REP NAME

DATE

ANNEX Part A

The following measures have been implemented by both the Controller and the Processor

Compliance with Article 32, para 1 of GDPR

50. Consideration of anonymisation, pseudonymisation and encryption of all data and the implementation of such measures where appropriate;

51. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and related services;

52. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

53. A process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of the processing;

Compliance with Article 32, para 2 of GDPR

54. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented

by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to data transmitted, stored or otherwise processed;

Compliance with Article 32, para 3 of GDPR

55. Adherence to an approved code of conduct referred to in Article 40 (GDPR) or an approved certification mechanism as referred to in Article 42 (GDPR) may be used as an element by which to demonstrate compliance with the requirements set out in para 1 of GDPR – see above;

Compliance with Article 32, para 4 of GDPR

56. The Controller will ensure that anyone acting on their behalf does not process any of the Data unless following instructions from the Controller unless they are required to do so under English law;

57. The Processor will ensure that anyone acting on their behalf does not process any of the Data unless following instructions from the Controller unless they are required to do so under English law;

ANNEX Part B

58. The Processor's Data Protection Representative shall be REP NAME or such other person as shall be notified by the Processor;

59. The Controller's Data Protection Representative shall be NAME or such other person as shall be notified by the Controller