

QWARIE FRAMEWORK DATA PROCESSING AGREEMENT

Table of Contents

1.0 INTRODUCTION.....	2
2.0 DEFINITIONS.....	2
3.0 COMPLIANCE WITH APPLICABLE LAWS.....	2
4.0 DATA CONTROLLER / DATA PROCESSOR.....	3
5.0 AUTHORITY TO DISCLOSE.....	3
6.0 AUTHORITY TO PROCESS.....	3
7.0 ACCEPTANCE.....	4
8.0 ACTION ON INSTRUCTION.....	4
9.0 OWNERSHIP.....	4
10.0 DATA QUALITY.....	5
11.0 DATA PROCESSING REGISTER.....	5
12.0 CONFIDENTIALITY.....	5
13.0 BEST PRACTICE.....	5
14.0 DATA PROCESSOR EMPLOYEE CONFIDENTIALITY & TRAINING.....	6
15.0 PERSONAL DATA SECURITY & MONITORING.....	6
16.0 TRANSFER OF DATA.....	7
17.0 RETURN, RETENTION AND DELETION POLICIES.....	7
18.0 RESTORE SERVICE.....	7
19.0 SECURITY BREACHES AND INCIDENTS.....	8
20.0 REQUEST FOR DISCLOSURE FROM A DATA SUBJECT.....	8
21.0 INSPECTION RIGHTS.....	9
22.0 INDEMNITY & LIABILITY.....	9
23.0 BREACH OF THIS AGREEMENT & CONSEQUENCES.....	9
24.0 VARIATION AND VERSIONING.....	9
25.0 TERMINATION.....	10
26.0 SURVIVAL OF THE AGREEMENT.....	10
27.0 GOVERNING LAW.....	10
APPENDIX 1.....	11

1.0 INTRODUCTION

- 1.1 This Framework Data Processing Agreement, between the Data Processor and the Data Controller, sets out the obligations and responsibilities for compliance with the Data Protection Act (DPA) 2018 in respect of the disclosure and processing of Personal Data in the matter of OSINT(Open Source Intelligence) research, where;
 - 1.1.2 the Data Processor shall process the Personal Data of a Data Subject with publicly available information as instructed by the Data Controller.
- 1.2 Where the Parties might agree to amend this Agreement, so that it shall become mutual, this Framework Agreement shall provide the basis for a mutual agreement.
- 1.3 This Agreement shall not confer on any Party, a commercial advantage or disadvantage, so that this Agreement is equitable under the law and is for the sole purpose of compliance with the prevailing data protection legislation.
- 1.4 This Framework Agreement shall rely upon further documentation set out in Appendix 1.

2.0 DEFINITIONS

- 2.1 Words and phrases in this Agreement shall have the meanings given to them in the Data Protection Act 2018.
- 2.2 Agreement: this Framework Data Processing Agreement.
- 2.3 Data protection legislation shall mean:-
 - 2.3.1 the Data Protection Act 2018, and;
 - 2.3.2 regulations made under DPA 2018.
- 2.4 Data Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
- 2.5 Data Processor: the legal entity which processes personal data on behalf of the Data Controller.
- 2.6 Data Subject: the individual to whom Personal Data relates.
- 2.7 Instruction: the written, documented instruction, issued by the Data Controller to the Data Processor, and directing the Data Processor to perform the processing in compliance with article 4.5 of this Agreement.
- 2.8 Party: the Data Controller and the Data Processor.

3.0 COMPLIANCE WITH APPLICABLE LAWS

- 3.1 In relation to the processing of Personal Data as set out in Section 1 of this Agreement;

- 3.2 the Data Processor covenants, warrants and undertakes to comply with all applicable laws, regulations and guidelines provided by the authorities within the jurisdiction, including, but not limited to, the DPA 2018, and where;
- 3.3 there might be any amendment, instrument, supplement, replacement and/or any other modification, that from time to time shall apply to the legal framework, so that;
- 3.4 this Agreement shall remain in force without modification, unless the Parties agree, to a modified agreement, in writing.

4.0 DATA CONTROLLER / DATA PROCESSOR

- 4.1 The Data Controller processes Personal Data in connection with its business activities.
- 4.2 The Data Processor processes Personal Data on behalf of other businesses and organisations, and;
 - 4.2.1 in compliance with Article 115 of the DPA 2018, the Data Processor is registered with the Information Commissioner Officer.
- 4.3 The Data Controller wishes to engage the services of the Data Processor to process Personal Data on its behalf.
- 4.4 The Data Controller shall determine the purposes for which and the manner in which its Personal Data shall be Processed by the Data Processor.
- 4.5 The manner in which all Personal Data disclosed by the Data Controller shall be processed by the Data Processor shall be in line with OSINT techniques.

5.0 AUTHORITY TO DISCLOSE

- 5.1 The Data Controller warrants that:-
 - 5.1.1 it shall comply with its obligations as a controller, under Article 61 (2) (i) of the DPA 2018, in respect of its processing and disclosure of Personal Data, and any processing Instructions it might issue to the Data Processor, and;
 - 5.1.2 it has provided notice and obtained (or shall obtain) all consents and rights necessary under applicable data protection legislation for the Data Processor to process Personal Data on its behalf.
- 5.2 Prior to remitting an Instruction to the Data Processor, the Data Controller is required to determine and document the lawful basis for the processing of Personal Data relating to the Data Subject, so that;
- 5.3 where the Data Controller shall remit an Instruction to the Data Processor, it is tacitly implied that the legal basis for the processing of Personal Data, relating to the Data Subject, has been documented in compliance with applicable data protection legislation.

6.0 AUTHORITY TO PROCESS

- 6.1 Article 59 (2) of the DPA 2018 provides that:

“The controller may use only a processor who provides guarantees to implement appropriate technical and organisational measures that are sufficient to secure that the processing will—

- (a) meet the requirements of this Part, and
- (b) ensure the protection of the rights of the data subject.”

6.2 Article 59 (5) of the DPA 2018 requires that:

“The processing by the processor must be governed by a contract in writing between the controller and the processor.”

6.3 Article 59 (6) (a) of the DPA 2018 requires that:

“The contract must, in particular, provide that the processor must—
(a) act only on instructions from the controller”

6.4 In compliance with the above-mentioned provisions of Article 59 of the DPA 2018, the Controller and Processor shall enter into this Data Processing Agreement.

7.0 ACCEPTANCE

7.1 Acceptance of this Agreement is disclosure of an Instruction by the Data Controller to the Data Processor, or by other means that might be a signature or acknowledgement by e-mail.

7.2 The date of the Agreement is the date that the first Instruction is remitted to the Data Processor.

7.3 Where the Data Controller does not agree to be bound by this Agreement, the Data Controller cannot remit any Instruction to the Data Processor.

8.0 ACTION ON INSTRUCTION

8.1 In compliance with Article 60 (a) of the DPA 2018, the Data Processor, and any person under the authority of the Data Processor, shall process Personal Data, only upon documented Instruction of the Data Controller.

8.2 Where the Data Controller remits to the Data Processor an Instruction to process the data of a Data Subject, the authority to process the Personal Data is conveyed to the Data Processor, and;

8.3 where the authority is not explicit within an Instruction, the authority is implicit as conferred by this Agreement, so that;

8.4 the Instruction shall authorise the Data Processor to perform processing activities as set out in Article 1.2 of this Agreement, and where;

8.5 the authority passed to the Data Controller shall remain active throughout the commercial relationship between the Parties.

9.0 OWNERSHIP

The Data Processor shall make no claim to any right or title of the Personal Data that is disclosed to the Data Processor by the Data Controller.

10.0 DATA QUALITY

- 10.1 Personal Data shall relate to the Data Subject(s) identified in the Instruction of the Data Controller.
- 10.2 The Data Processor is obliged to process all publicly available Personal Data with care and diligence, so that the Data Controller might rely of the quality of the Personal Data.
- 10.3 Where the Data Controller processes personal information prior to disclosure to the Data Processor, so that the processed information is included in the Instruction of the Data Controller, the Data Processor has the right to rely on that Personal Data.
- 10.4 Where the quality of the Personal Data within an Instruction is not accurate, so that the Personal Data does not relate to the Data Subject(s) within the Instruction, see article 22.3 of this Agreement.

11.0 DATA PROCESSING REGISTER

- 11.1 The Data Processor maintains and stores a single register of all data processing activities performed by the Data Processor.
- 11.2 Within the register, one row relates to one Instruction received and processed by the Data Processor.
- 11.3 The Data Processor shall not disclose Personal Data within the register, that relates to services supplied to other parties.
- 11.4 Should the Data Controller require a copy of the register, the Data Processor shall select and remit to the Data Controller, the Instructions within the register, that relate only to the Data Controller.

12.0 CONFIDENTIALITY

- 12.1 Personal Data acquired by the Data Controller and passed by the Data Controller to the Data Processor is confidential.
- 12.2 Personal Data acquired by the Data Processor, through the performance of its research activity, and passed to the Data Controller is confidential.
- 12.3 The Data Processor shall not make any use of any Personal Data disclosed by the Data Controller otherwise than in connection with the provision of the services as set out in article 1.2 of this Agreement.
- 12.4 The Data Processor covenants, warrants and undertakes to keep in confidence the Personal Data, that is disclosed by the Data Controller.

13.0 BEST PRACTICE

- 13.1 The Data Processor has adopted the Best Practice Guidance developed by the Chartered Insurance Institute New Generation Group 2013.

- 13.2 This document sets out industry Best Practice Guidance for making and responding to requests for disclosure made under Schedule 2, Part 1 Paragraph 2 of the Data Protection Act 2018.
- 13.3 Schedule 2, Part 1 Paragraph 2 of the Data Protection Act 2018 includes an exemption to the non-disclosure provisions within the General Data Protection Regulation 2016/679, and allows an organisation to disclose Personal Data to a third party, where the disclosure and processing of Personal Data is for one of the following purposes:-
- 13.3.1 the prevention or detection of crime, or;
- 13.3.2 the apprehension or prosecution of offenders, or;
- 13.3.3 the assessment or collection of any tax or duty or of any imposition of a similar nature, and;
- 13.4 where the application of the non-disclosure provisions in relation to the disclosure in question would be likely to prejudice any of the three purposes mentioned above.
- 13.5 The Best Practice Guidance is listed in Appendix 1 of this Agreement.

14.0 DATA PROCESSOR EMPLOYEE CONFIDENTIALITY & TRAINING

- 14.1 Each employee of the Data Processor is bound by a signed employment contract and confidentiality contract.
- 14.2 All policies and procedures that relate to activities performed by employees are disclosed to new employees during their induction, and to all employees at any periodic review, where the employee is obliged to review the policy, and sign off on their obligation to comply.
- 14.3 During the induction phase of employment, each new employee receives training related specifically to data protection and the security and confidentiality processes and protocols implemented and enforced by the Data Processor, so that;
- 14.4 each employee shall perform their duties and obligations in a manner consistent with this Agreement, and so that the Data Processor shall comply with this Agreement.

15.0 PERSONAL DATA SECURITY & MONITORING

- 15.1 The Data Processor hereby warrants and guarantees that it has implemented appropriate technical and organisational measures which relate to the security of processing of Personal Data, so that processing shall meet the requirements of the DPA 2018, and;
- 15.2 the Data Processor hereby warrants that it has taken, and shall continue to take all measures required pursuant to DPA 2018 to ensure the protection of the rights of Data Subjects.
- 15.3 For the full extent of the security measures implemented by the Data Processor, see Appendix 1 of this Agreement.

16.0 TRANSFER OF DATA

- 16.1 The Data Controller is obliged to provide a secure file exchange service between the Parties, however;
- 16.2 where the Data Controller is unable to do so, the Data Processor shall offer to the Data Controller the use of its secure data transfer option, that is download from the secure server of the Data Processor.

17.0 RETURN, RETENTION AND DELETION POLICIES

- 17.1 As directed by the Data Controller, the Data Processor shall safely and securely return to the Data Controller any document in its possession that contains Personal Data disclosed by the Data Controller.
- 17.2 All documents or files containing Personal Data are held by the Data Processor in electronic format, so that no Personal Data disclosed by the Data Controller is ever retained on paper or printed.
- 17.3 The Data Processor shall retain any documents that contain Personal Data until such time that consideration has been provided by the Data Controller.
- 17.4 Within 3 days of receipt of payment that relates to the processing event, the Data Processor shall delete from its servers:-
- 17.4.1 any document containing Personal Data disclosed by the Data Controller, and;
- 17.4.2 all e-mail communication relating to an Instruction remitted by the Data Controller.
- 17.5 The Data Processor operates an internal and secure local data backup.
- 17.5.1 A restore service is available to the Data Controller on demand, see section 18 of this Agreement, and within the term, see clause 17.7 of this Agreement.
- 17.6 Documents and e-mails are purged from the backup, by an automated process.
- 17.7 Documents and e-mails containing Personal Data of the Data Controller are purged from backup three months from the date that consideration has been provided by the Data Controller.
- 17.8 The Data Controller may request exclusion from the backup process, so that Personal data is deleted in compliance with article 17.4, and not saved to backup.

18.0 RESTORE SERVICE

- 18.1 Where the Data Controller might have misplaced a case bundle, within 3 months of the payment date, see clause 17.4, the Data Controller might request a restore of a case bundle from the Data Processor's backup.
- 18.2 The restore service is free of charge.

19.0 SECURITY BREACHES AND INCIDENTS

19.1 The Data Processor shall comply with its obligations as listed in Article 108 (1) and (2) DPA 2018 :-

“(1) If a controller becomes aware of a serious personal data breach in relation to personal data for which the controller is responsible, the controller must notify the Commissioner of the breach without undue delay.

(2) Where the notification to the Commissioner is not made within 72 hours, the notification must be accompanied by reasons for the delay.”

19.2 For the purposes of this section, a personal data breach is serious if the breach seriously interferes with the rights and freedoms of a data subject, as defined in Article 108 (7) DPA 2018.

19.3 In compliance with Article 108 (5) DPA 2018 “If a processor becomes aware of a personal data breach (in relation to data processed by the processor), the processor must notify the controller without undue delay.”

19.3.1 the Data Processor agrees to notify the Data Controller within 72 hours of becoming aware of any incident or breach of its security obligations in accordance the DPA 2018, where;

19.3.2 the incident or breach might result in the unauthorised access, unauthorised disclosure, misuse, loss, theft, or accidental or unlawful destruction, alteration and/or loss of any Personal Data disclosed by the Data Controller.

19.4 Notice to the Data Controller of a Data Security incident or Data Breach, shall be delivered in writing, to the e-mail address supplied by the Data Controller.

19.5 In the event of a Data Security incident or Data Breach, the Data Processor shall promptly take adequate remedial measures to mitigate the effects and to minimise any damage resulting from the Data Security incident or Data Breach, and;

19.6 The Data Processor shall provide such information, in relation to the Data Security incident or Data Breach, to the Data Controller.

19.7 The Data Processor shall fully cooperate with the Data Controller to develop and execute a response that shall address the Data Security incident or Data Breach, and;

19.8 the Data Processor shall cooperate with the Data Controller to adequately inform any Data Subject or other person affected by the data incident or Data Breach.

19.9 Please see the Data Breach Policy of the Data Processor listed in Appendix 1 of this Agreement.

20.0 REQUEST FOR DISCLOSURE FROM A DATA SUBJECT

20.1 The Data Processor warrants and undertakes to assist the Data Controller in the fulfilment of the Data Controller's obligation to respond to a request by a Data Subject to access all their Personal Data under the rights conferred upon them by data protection legislation.

20.2 In the unlikely event that the Data Processor is in the possession of a partially performed Instruction, when the request for disclosure is received by the Data Controller, the Data processor shall disclose the information in its possession, and shall disclose the relevant record from the Data Processor's Register, as set out in Section 11 of this Agreement.

21.0 INSPECTION RIGHTS

21.1 The Data Controller has the right to present at the facility of the Data Processor, so that;

21.1.1 the Data Controller, may inspect any material containing Personal Data that relates to their business, and;

21.1.2 the Data Controller might verify the security procedures implemented by the Data Processor.

21.2 In this matter, the Data Processor shall comply with the demands of the Data Controller.

21.3 The Data Processor shall be obliged to comply with the Data Processor's access policy.

22.0 INDEMNITY & LIABILITY

22.1 The Data Processor shall indemnify, and keep the Data Controller indemnified to the fullest extent permitted by law, in respect of any actions, claims, costs, damages, (including damages or compensation paid by the Data Controller on the advice of its relevant parties to settle any action), expenses (including legal or other expenses), fines, penalties, sanctions, settlement or any other enforcement action that is imposed on the Data Controller by any court of competent jurisdiction or regulatory or enforcement authority, arising from a breach and/or potential breach of data protection legislation by the Data Processor whatsoever or howsoever arising.

22.2 In relation to any Data Breach and/or potential breach regarding Personal Data processed by the Data Processor, in relation to the provision of services to the Data Controller, the Data Processor's liability shall not exceed the value of two million pounds sterling (£2,000,000) for each collective breach.

22.3 The Data Controller shall be liable to the Data Processor for the cost of processing any erroneous Instruction with inaccurate or misleading Personal Data, and;

22.4 the Data Processor shall have the right to recover from the Data Controller, the cost of processing any erroneous Instruction.

23.0 BREACH OF THIS AGREEMENT & CONSEQUENCES

Where a Party shall commit a breach of this Agreement, the Party in breach shall be liable under section 22 of this Agreement.

24.0 VARIATION AND VERSIONING

24.1 The Data Processor may, at any time, make any variation to this Agreement.

- 24.2 The variation shall incur a version number that shall reflect the magnitude of the variation.
- 24.3 Where there shall be a variation to the material or meaning of this Agreement, the version shall incur a prime number change.
- 24.4 Where a variation correction shall be a minor correction of syntax, spelling or grammar, with no material effect, the version shall incur a decimal number.
- 24.5 Where the Data Processor shall apply a substantial variation to this Agreement, the Data Processor shall advise the Data Processor of the variation and shall make available the current version of this Agreement.
- 24.6 The Data Processor shall publish the current version of this Agreement on its website, and;
- 24.7 the Data Processor shall provide a link to the current version of this Agreement in all e-mail communication, so that;
- 24.8 the Data Controller may view the current version of this Agreement by following the link in the signature file of any e-mail remitted by the Data Processor.

25.0 TERMINATION

- 25.1 This Agreement shall terminate at the end of the commercial relationship between the Parties.

26.0 SURVIVAL OF THE AGREEMENT

The obligations, undertaking and acknowledgments set out in this Agreement shall survive the termination or conclusion of this Agreement.

27.0 GOVERNING LAW

- 27.1 This Framework Agreement shall be governed by, and construed in accordance with, English law.
- 27.2 The Parties shall acknowledge and agree that any dispute or claim arising out of or in connection with this Agreement, or its subject matter or formation (including non-contractual disputes or claims), shall be governed by the courts of England and Wales.
- 27.3 The Parties shall attempt to resolve any dispute arising out of, or relating to this Agreement, through negotiations between appointed representatives who have the authority to settle such disputes, and;
- 27.4 where negotiations shall fail, the Parties shall engage the services of a Third Party mediator to settle any such disputes through confidential mediation.
-

APPENDIX 1

1. Policies and Procedures relevant to this Agreement available at <https://www.qwarie.com/documents>

- Research Privacy Policy
- Security Policy
- Data Breach Policy
- Modern Slavery Policy
- Equality and Diversity Policy
- Anti-Bribery Policy
- Corporate and Social Responsibility Policy
- Complaints Policy and Procedure
- Health & Safety Policy
- Cookie Policy
- Best Practice Guide: Schedule 2, part 1 Paragraph 2 of the Data Protection Act 2018

2. Data protection legislation relevant to this Agreement available at http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf