QWARIE FRAMEWORK DATA PROTECTION AGREEMENT

Table of Contents

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 General Data Protection Regulation 2016/679 (GDPR) 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 GDPR.

2.2 Agreement: this Framework Data Processing Agreement.

2.3 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.

2.4 Data Processor: the legal entity which processes personal data on behalf of the Data Controller.

2.5 Data Subject: the individual to whom Personal Data relates.

2.6 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.

2.7 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 and regulations within the jurisdiction of this Agreement, including but not limited to, the GDPR, and where;

3.3 there might be any amendment, supplement, replacement and/or any 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.

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 LEGAL BASIS FOR PROCESSING

5.1 The Data Controller has the right to process Personal Data in compliance with article 6.1 (f) of GDPR:

"Processing shall be lawful only if and to the extent that at least one of the following applies:
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

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 ACCEPTANCE

6.1 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.

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

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

7.0 ACTION ON INSTRUCTION

7.1 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.

7.2 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;

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

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

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

8.0 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.

9.0 DATA QUALITY

9.1 Personal Data shall relate to the Data Subject(s) identified in the Instruction of the Data Controller.

9.2 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.

9.3 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.

9.4 Where the quality of the Personal Data within an Instruction is not accurate, so that the Personal Data does not apply to the Data Subject(s) is included within the Instruction, see article 20.3 of this Agreement.

10.0 DATA PROCESSING REGISTER

10.1 The Data Processor maintains and stores a single register of all data processing activities performed by the Data Processor.

10.2 Within the register, one row relates to one Instruction received and processed by the Data Processor.

10.3 The Data Processor shall not disclose Personal Data within the register, that relates to services supplied to other parties.

10.4 Should the Data Controller require a copy of the register, the Data Processor shall select and remit to the Data Controller, the personal information within the register, that relates only to the Data Controller.

11.0 CONFIDENTIALITY

11.1 Personal Data acquired by the Data Controller and passed by the Data Controller to the Data Processor is confidential.

11.2 Personal Data acquired by the Data Processor, through the performance of its research activity, and disclosed to the Data Controller is confidential.

11.3 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.

11.4 The Data Processor covenants, warrants and undertakes to keep in confidence the Personal Data, that is disclosed by the Data Controller.

12.0 DATA PROCESSOR EMPLOYEE CONFIDENTIALITY & TRAINING

12.1 Each employee of the Data Processor is bound by a signed employment contract and confidentiality contract.

12.2 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.

12.3 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;

12.4 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.

13.0 PERSONAL DATA SECURITY & MONITORING

13.1 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 GDPR, and;

13.2 the Data Processor hereby warrants that it has taken, and shall continue to take all measures required pursuant to GDPR to ensure the protection of the rights of Data Subjects.

13.3 For the full extent of the security measures implemented by the Data Processor, see Appendix 1 of this Agreement.

14.0 TRANSFER OF DATA

14.1 The Data Controller shall have the obligation to provide secure file exchange between the Parties, however;

14.2 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.

15.0 RETURN, RETENTION AND DELETION POLICIES

15.1 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.

15.2 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.

15.3 The Data Processor shall retain any documents that contain Personal Data until such time that consideration has been provided by the Data Controller.

15.4 Within 3 days of receipt of payment that relates to the processing event, the Data Processor shall delete from its servers:-

15.4.1 any document containing Personal Data disclosed by the Data Controller, and;

15.4.2 all e-mail communication relating to an Instruction remitted by the Data Controller.

15.5 The Data Processor operates an internal and secure local data backup.

15.5.1 A restore service is available to the Data Controller on demand, see section 16 of this Agreement, and within the term, see clause 15.7 of this Agreement.

15.6 Documents and e-mails are purged from the backup, by an automated process.

15.7 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.

15.8 The Data Controller may request exclusion from the backup process, so that Personal data is deleted in compliance with article 15.4, and not saved to backup.

16.0 RESTORE SERVICE

16.1 Where the Data Controller might have misplaced a case bundle, within 3 months of the payment date, see clause 15.4, the Data Controller might request a restore of a case bundle from the Data Processor's backup.

16.2 The restore service is free of charge.

17.0 SECURITY BREACHES AND INCIDENTS

17.1 Article 33 (2) GDPR states: "The processor shall notify the controller without undue delay after becoming aware of a personal data breach", therefore;

17.2 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 GDPR, where;

17.3 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.

17.4 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.

17.5 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;

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

17.7 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;

17.8 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.

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

18.0 REQUEST FOR DISCLOSURE FROM A DATA SUBJECT

18.1 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.

18.2 In the unlikely event that the Data Processor is in the possesion 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 posession, and shall disclose the relevant record from the Data Processor’s Register, as set out in Section 10 of this Agreement.

19.0 INSPECTION RIGHTS

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

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

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

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

19.3 The Data Processor shall be obliged to comply with the Data Processor’s access policy.

20.0 INDEMNITY & LIABILITY

20.1 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.

20.2 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 instance.

20.3 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;

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

21.0 BREACH OF THIS AGREEMENT & CONSEQUENCES

Where a Party shall commit a breach of this Agreement, the Party in breach shall be liable under section 20 of this Agreement.

22.0 VARIATION AND VERSIONING

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

22.2 The variation shall incur a version number that shall reflect the magnitude of the variation.

22.3 Where there shall be a variation to the material or meaning of this Framework Contract, the version shall incur a prime number change.

22.4 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.

22.5 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.

22.6 The Data Processor shall publish the current version of this Agreement on its website, and;

22.7 the Data Processor shall provide a link to the current version of this Agreement in all e-mail communication, so that;

22.8 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.

23.0 TERMINATION

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

24.0 SURVIVAL OF THE AGREEMENT

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

25.0 GOVERNING LAW

25.1 This Agreement shall be governed by, and construed in accordance with, English law.

25.2 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, however;

25.3 the courts of England and Wales shall have no exclusive right or governance or jurisdiction.

25.4 This Agreement might be efficiently and conveniently interpreted, so that;

25.5 it might comply with the laws of contract, in another jurisdiction.

25.6 There shall be no exclusive submission to the jurisdiction of the courts of England and Wales, so that;

25.7 the rights of either Party to bring proceedings in another competent court in another jurisdiction, shall not (and shall not be construed as) limited by jurisdiction, so that;

25.8 either Party might rely on the competent judicial authority in the registered jurisdiction of either Party.

25.9 The jurisdiction of the Agreement shall apply to legal entities and naturalised persons in any jurisdiction.

25.10 The Parties shall attempt to resolve any dispute arising out of or relating to the Agreement, through negotiations between appointed representatives who have the authority to settle such disputes, and;

25.11 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 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679