

GENERAL DATA PROTECTION REGULATION (EU) 2016/679 AGREEMENT

between

The Data Controller:

Company Registration:

ICO or other registration:

and

The Data Processor: Qwarie Ltd. Rumwell Hall, Rumwell, Taunton, Somerset, TA4 1EL UK

Company Registration: 10113351

ICO Registration: A8124343

Where each is a “Party” and together they are the “Parties” to this, “GDPR Agreement”.

Table of Contents

3.0 DECLARATION BY THE DATA PROCESSOR - QWARIE GROUP 2

4.0 COMPLIANCE WITH APPLICABLE LAWS 3

5.0 DEFINITIONS 3

6.0 DATA CONTROLLER / DATA PROCESSOR..... 3

7.0 LEGAL BASIS..... 3

8.0 ACCEPTANCE..... 4

9.0 CONFIDENTIALITY 4

10.0 DISCLOSURE..... 5

11.0 PERSONAL DATA SECURITY & MONITORING 5

12.0 SECURITY BREACHES AND INCIDENTS..... 6

13.0 OWNERSHIP 6

14.0 ORIGINALS & COPIES 7

15.0 DATA TRANSFER 7

16.0 RETENTION / RETURN 7

17.0 DELETION POLICY 7

18.0 DATA QUALITY 8

19.0 DATA PROTECTION REGISTRATION 8

20.0 INSPECTION RIGHTS 8

21.0 EMPLOYEE CONFIDENTIALITY & TRAINING 9

22.0 INDEMNITY & LIABILITY 9

23.0 ACTION ON INSTRUCTION 9

24.0 DATA SUBJECT REQUESTS 10

25.0 NO REPRESENTATION..... 10

26.0 DATA PROCESSING REGISTER..... 10

27.0 BREACH OF THIS AGREEMENT & CONSEQUENCES 10

28.0 TERMINATION & VARIATION 10

29.0 SURVIVAL OF TERMINATION 10

30.0 GOVERNING LAW 11

APPENDIX 1 12

- 2.1 This GDPR Agreement governs the arrangements, relating to the transfer and processing of Personal Data between the Parties.
- 2.2 In a transparent manner, the Parties wish to record their rights, obligations and commitments under this GDPR Agreement, to demonstrate their compliance with the GDPR, so that;
- 2.3 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 legislation.
- 2.4 Specifically, this agreement shall relate to the control and processing of personal information in the matter of OSINT research where the Data Processor shall process the Personal Data of a Data Subject with publicly available information.
- 2.5 Personal Data shall be disclosed by the Data Controller to the Data Processor in the form of a confidential and written instruction, and;
- 2.6 the Data Processor shall disclose Personal Data to the Data Controller by way of a confidential and written report, with the option to supply a complete case bundle that is the outcome of the processing activity.

3.0 DECLARATION BY THE DATA PROCESSOR - QWARIE GROUP

- 3.1 Qwarie Group is two companies, Qwarie Ltd and Qwarie EMEA SRL.
- 3.2 Qwarie EMEA SRL is an EU registered company that might provide resources to the legal Data Processor Qwarie Ltd.
- 3.3 So that, services performed by the Data Processor are delivered with resources provided by Qwarie EMEA SRL, under a Qwarie Group general service contract.
- 3.4 Qwarie EMEA SRL has one customer, that is the Data Processor.
- 3.5 At no time shall the Qwarie Group sub-contract any data processing activity to any other party.
- 3.6 The Data Processor recognises that it is accountable for processing the data, and for the delivery of the service, and that accountability is not assigned to Qwarie EMEA SRL.
- 3.7 Where a new Qwarie company might be incorporated and become part of the Qwarie Group, the Data Processor is obliged to disclose to the Data Controller the new entity, so that this GDPR Agreement might be amended.

Hereby, it is agreed that in:**4.0 COMPLIANCE WITH APPLICABLE LAWS**

- 4.1 In relation to the processing of Personal Data for the provision of the services as set out in Section 2 of this GDPR Agreement;
- 4.2 each Party covenants, warrants and undertakes to the other Party to comply with all applicable laws and regulations within the jurisdiction of this GDPR Agreement, including but not limited to, the GDPR, and where;
- 4.3 there might be any amendment, supplement, replacement and/or any modification, from time to time, to the applicable laws or regulations, including the GDPR, so that;
- 4.4 this GDPR Agreement shall remain in force without modification, unless the Parties agree, to a modified agreement, in writing.
- 4.5 the Parties agree to be aware of and to comply with all of their obligations under GDPR, so that;
- 4.6 the Parties shall perform their respective activity, so that the activity is in compliance with the GDPR.

5.0 DEFINITIONS

- 5.1 Words and phrases in this GDPR Agreement shall have the meanings given to them in Article 4 of the GDPR.
- 5.2 The customer is the customer of the Data Controller that is the Data Subject.

6.0 DATA CONTROLLER / DATA PROCESSOR

- 6.1 The Parties acknowledge and agree that, in respect of all Personal Data controlled by the Data Controller, the Data Controller shall determine the purposes for which and the manner in which Personal Data will be Processed by the Data Processor.
- 6.2 The manner in which all Personal Data controlled by the Data Controller shall be processed by the Data Processor shall be in line with OSINT (Open Source Intelligence) techniques.

7.0 LEGAL BASIS

- 7.1 Article 6.1 (f) of GDPR grants the Data Controller the right to process Personal Data, where;
- 7.2 the processing of Personal Data is necessary for the purpose of a legitimate interest pursued by the Data Controller, so that;
- 7.3 the Data Controller has the lawful basis to investigate a Data Subject where the purpose is explicit and legitimate.

- 7.4 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;
- 7.5 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 the GDPR.
- 7.6 Where the Data Controller remits to the Data Processor an instruction to process the data of the Data Subject, the authority to process the Personal Data is passed to the Data Processor, and;
- 7.7 where the authority is not explicit within an instruction, the authority is implicit as conferred by this agreement, so that;
- 7.8 the instruction shall authorise the Data Processor to perform activities as set out in Article 2.4 of this agreement, and where;
- 7.9 the authority acquired by the Data Controller shall remain active throughout the commercial relationship between the Parties.

8.0 ACCEPTANCE

- 8.1 Where the Data Controller is in possession of this agreement, but has elected to not sign this agreement, the subsequent remission of any instruction by the Data Controller to the Data Processor, after the date of notification of this agreement by the Data Processor shall indicate, for all legal purposes that the Data Controller is bound by this GDPR Agreement.
- 8.2 The signature and date of acceptance of the Data Processor is not required on this GDPR Agreement, so that this GDPR Agreement might be enforced by either party.
- 8.3 The date of the agreement is the date that the first instruction is remitted to the Data Processor.
- 8.4 Where the Data Controller does not agree to be bound by this agreement, the Data Controller cannot remit any instruction to the Data Processor.

9.0 CONFIDENTIALITY

- 9.1 Personal Data acquired by the Data Controller and passed by the Data Controller to the Data Processor is confidential.
- 9.2 Personal Data acquired by the Data Processor, through the performance of its research activity, and passed to the Data Controller is confidential.
- 9.3 Both Parties acknowledge that any breach of confidentiality might expose the Data Controller to reputational damage, pecuniary liability to the individuals whose data is compromised, and fines from the appropriate authority.

- 9.4 Hereby, both the Data Controller and the Data Processor covenant, warrant and undertake to keep in confidence the Personal Data, that is controlled by the Data Controller.

10.0 DISCLOSURE

- 10.1 Where Personal Data is disclosed by the Data Controller to the Data Processor, the Data Processor is obliged to maintain the confidentiality of the Personal Data, so that the Data Processor shall not disclose the personal information to any other party and shall maintain secure systems that protect the Personal Data, and;
- 10.2 after the Data Processor has processed the personal information, and acquired additional personal information, that is disclosed to the Data Controller, the Data Controller is obliged to maintain the confidentiality of the Personal Data, so that the Data Controller shall maintain secure systems that protect the Personal Data. However;
- 10.3 the Data Controller does reserve the right to disclose the Personal Data to third parties that might be a law enforcement agency, a legal or accounting service provider or a private investigation service supplier, and that the disclosure shall comply with the GDPR.

11.0 PERSONAL DATA SECURITY & MONITORING

- 11.1 Where Personal Data is processed on behalf of the Data Controller, the Data Processor hereby warrants and guarantees that it has implemented appropriate technical and organisational measures, in such a manner that processing will meet the requirements of GDPR, and the Data Processor ensures the protection of the rights of Data Subjects as defined under the GDPR.
- 11.2 The Data Processor hereby warrants that it has taken, and will continue to take all measures required pursuant to GDPR which relate to the security of processing of Personal Data. This includes the implementation of appropriate technical and organisational measures to ensure a high level of security appropriate to the risk, including:
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
 - maintaining a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
 - implementation of appropriate measures in relation to the risks that the processing presents, and to protect against unauthorised access to, or unauthorised alteration, disclosure, loss or destruction of any Personal Data transmitted, stored or otherwise processed, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing;
 - implementation of adequate security programs and procedures to ensure that unauthorised persons will not have access to the equipment the Data Processor deploys to process Personal Data;
 - encryption of Personal Data where appropriate;
 - and where appropriate, the pseudonymisation of Personal Data allowed for under GDPR.

- 11.3 The Personal Data of the Data Controller is managed and reported separately from the Personal Data of any customer of the Data Controller, with the exception of the Data Processor's Register as outlined in Section 26 of this agreement.
- 11.4 The Data Processor shall maintain a robust and effective system to monitor all of its technical services for the detection of any anomalies and potential breaches of the Data Processor's obligations, under this GDPR Agreement.
- 11.5 For the fuller extent of the security measures implemented by the Data Processor, refer to appendix 1 of this GDPR Agreement.

12.0 SECURITY BREACHES AND INCIDENTS

- 12.1 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 with art. 33 (2) GDPR, where;
- 12.2 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 under the control of the Data Controller.
- 12.3 Notice to the Data Controller of a Data Security incident or Data Breach, shall be made by the Data Processor to the Data Protection Officer of the Data Controller.
- 12.4 The notice shall be delivered in writing, to the e-mail address supplied by the Data Controller.
- 12.5 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;
- 12.6 The Data Processor shall provide such information, in relation to the Data Security incident or Data Breach, to the Data Controller.
- 12.7 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;
- 12.8 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.
- 12.9 The Data Breach Policy of the Data Processor is available through Appendix 1 of this GDPR agreement.

13.0 OWNERSHIP

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

14.0 ORIGINALS & COPIES

- 14.1 The Data Processor hereby agrees not to make or permit to be made any copies of or in any other way reproduce the Personal Data, save only to the extent strictly necessary for the provision of the Service.
- 14.2 Where the processing of the Personal Data is complete, the Data Processor shall not store any Personal Data on a local computer, so that;
- 14.3 original e-mail instructions are stored on the server of the Data Processor, and original reports are transferred to and stored on the server of the Data Processor, until deleted in compliance with the Deletion Policy of the Data Processor.

15.0 DATA TRANSFER

- 15.1 The Data Controller shall have the obligation to provide secure file exchange between the Parties, however;
- 15.2 where the Data Controller is unable to do so, the Data Processor shall supply a secure data transfer option.

16.0 RETENTION / RETURN

- 16.1 As directed by the Data Controller, the Data Processor shall safely and securely return to the Data Controller any permitted copies of a document with personal information in its possession.
- 16.2 The Data Processor shall delete all Personal Data in line with its Deletion Policy.
- 16.3 In this context, Personal Data is all documents or files containing Personal Data, held by the Data Processor in electronic and printed format.
- 16.4 Where the Data Controller might instruct the Data Processor to perform further processing of a case that is closed, the Data Controller is obliged to return to the Data Processor the original report that shall have been deleted from the servers of the Data Processor.
- 16.5 The Processor is not obliged to return files that have undergone deletion and are yet to be purged from the backup. See section 17 of this GDPR Agreement.

17.0 DELETION POLICY

- 17.1 The Data Processor shall delete from its servers, any document containing Personal Data controlled by the Data Controller.
- 17.2 Deletion shall be performed within 3 days receipt of payment that relates to the processing event.
- 17.3 The Data Processor operates an internal and secure local data backup.
- 17.4 Documents are purged from the backup, by an automated process.

- 17.5 Document purge takes place three calendar months from the date that the file was last modified, which is the same day or the previous business day before the document was disclosed to the Data Controller.
- 17.6 The Data Controller may request exclusion from the backup process.
- 17.7 Where the Data Controller might request a restore of a case bundle from the Data Processor's backup, a fee of £100 for each case bundle restore shall be charged by the Data Processor.
- 17.8 Where the Data Processor has performed a deletion of any document containing Personal Data of the Data Controller, the Data Processor shall not be obliged to restore or return to the Data Controller any file from the backup, unless the Data Controller complies with article 17.7 of this GDPR Agreement.

18.0 DATA QUALITY

- 18.1 Personal Data shall relate to the Data Subject(s) identified in the instruction of the Data Controller.
- 18.2 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, so that;
- 18.3 Where the quantity of data processed is considerable, the Data Processor shall supply a summary of the data processed.
- 18.4 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.
- 18.5 Where the quality of the Personal Data within an instruction is not accurate, so that Personal Data that does not apply to the Data Subject(s) is included within the instruction, see article 22.3 of this GDPR Agreement.

19.0 DATA PROTECTION REGISTRATION

- 19.1 The GDPR abolishes the requirement to register for Data Protection with a supervisory authority, however;
- 19.2 the Data Processor is registered with the Information Commissioner Officer in the UK.
- 19.3 Any other company in the Qwarie Group complies with the Data Protection registration, obligations of the jurisdiction in which the company is registered.

20.0 INSPECTION RIGHTS

- 20.1 The Data Controller has the right to present at any Qwarie Group facility, so that,
- 20.2 any file, relating only to the Personal Data of the Data Controller, may be inspected.
- 20.3 In this matter, the Data Processor shall comply with the demands of the Data Controller.

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

21.0 EMPLOYEE CONFIDENTIALITY & TRAINING

21.1 Each employee of the Data Processor is bound by a signed employment contract and confidentiality contract, and where;

21.2 during the induction phase of employment, each new employee receives training related specifically to the GDPR and the security and confidentiality processes and protocols implemented and enforced by the employer, so that;

21.3 each employee shall read and understand the policies and other documents as set out in Appendix 1 of this GDPR Agreement, so that;

21.4 each employee shall perform their duties and obligations in a manner consistent with this GDPR Agreement, and so that the Data Processor shall comply with this agreement.

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 the GDPR 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 instance.

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 the erroneous instruction in compliance with Section 25 of this GDPR Agreement.

23.0 ACTION ON INSTRUCTION

23.1 The Data Processor warrants and undertakes to perform the processing of Personal Data only to the extent strictly required under this GDPR Agreement, and in accordance with the requirements of the GDPR.

23.2 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.

24.0 DATA SUBJECT REQUESTS

- 24.1 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 the GDPR.
- 24.2 In this event, the Data Processor shall disclose any partially performed case to the Data Controller and the relevant row from the Data Register, as set out in Section 26 of this GDPR Agreement.

25.0 NO REPRESENTATION

- 25.1 Where an instruction provided by the Data Controller might contain inaccurate Personal Data, and where the Data Processor is ordered to process the information, the Data Processor shall not be liable for the processing of inaccurate information.
- 25.2 The Data Processor shall have the right to seek consideration for processing inaccurate data supplied by the Data Controller.

26.0 DATA PROCESSING REGISTER

- 26.1 The Data Processor holds a single register of all data processing activities performed by Qwarie Group. The Data Processor shall not disclose Personal Data within the register, that relates to services supplied to other customers of the Data Processor.
- 26.2 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.

27.0 BREACH OF THIS AGREEMENT & CONSEQUENCES

Where a Party shall perform, or not perform an activity, so that that either or both Parties might be in breach of the GDPR and this agreement, the Party in breach shall be liable under section 22 of this GDPR Agreement.

28.0 TERMINATION & VARIATION

- 28.1 This GDPR Agreement may only be varied with the written consent of both Parties.
- 28.2 This GDPR Agreement shall terminate at the end of the commercial relationship between the Parties.

29.0 SURVIVAL OF TERMINATION

The Parties agree that the obligations, undertakings, agreements and acknowledgements set out in this GDPR Agreement shall survive the termination or conclusion of this GDPR Agreement.

30.0 GOVERNING LAW

This GDPR Agreement, and any dispute or claim arising out of, or in connection with it, or its subject matter or formation (including non-contractual disputes or claims) shall be governed by, and construed in accordance with, the laws of England.

Signed for and on behalf
of the Data Controller

Signed for and on behalf
of the Data Processor

Signature.....

Signature.....

Name.....

Name.....

Position.....

Position.....

Date.....

Date.....

APPENDIX 1

The Data Processor provides extensive documentation that includes:-

- Compliance Statement
- Data Protection Compliance Statement
- Customer Consent Personal Data Processing
- Notice of DPA Compliance
- Cookie Policy
- Data Breach Policy
- Modern Slavery Policy
- Research Privacy Policy

all available at <https://www.qwarie.com/documents>