Wintro – Data Processing Policy

Last update: May 2024

Pursuant to the Agreement, Wintro provides the Wintro Platform and the Service to the Customer. The provision of the Wintro Platform and the Service leads to the collection and processing of Personal Data by Wintro, in its capacity as a data processor, on behalf of the Customer. Therefore, Wintro provides the Customer with this Data Processing Policy ("**DPP**") which sets out (i) how Wintro shall manage, process and secure the Personal Data; as well as (ii) all parties' obligations to comply with the Privacy Legislation.

By concluding the Agreement with Wintro, the Customer has indicated that it has read, understands and accepts the terms and conditions of this DPP, which forms an integral part of said Agreement.

This DPP may be updated from time to time by Wintro, in which case Wintro shall notify the Customer through its or the Wintro Platform. In any event, the latest version of this DPP can always be accessed on the Website, as well as on the Wintro Platform.

You can find our (archived) Wintro DPPs here.

1 DEFINITIONS

1.1 Capitalized terms shall have the meaning as set out below.

Affiliate:	unless otherwise defined in the Agreement, a business entity that (in)directly controls, is controlled by or is under common control (i.e. the direct of ownership of more than 50% of the voting securities of a business entity) with such party;
Agreement:	the combined term for the **(i)** agreement; **(ii)** Wintro proposal; and **(iii)** additional orders, with the Customer;
Authorized Users:	individuals authorized by the Customer to have access to and make use of the Service and the Wintro Platform;
Customer Employee:	the Customer's employees of whom the professional network is accessed, through LinkedIn, and used to search matches for the Customer's open vacancies;
Customer:	the party with whom Wintro has concluded the Agreement, including its Affiliate(s);
Data Subject:	the natural person to whom the Personal Data relates, as described in **Annex I**;
Participating Affiliate:	an Affiliate of the Customer, which, although it has not entered into a separate Agreement with Wintro, has been authorized to access and use the Service under the existing Agreement between Wintro and the Customer;
Personal Data	personal data (within the meaning of Privacy Legislation) relating to the Data Subjects, as described in **Annex I**;
Privacy Legislation:	the (supra)national privacy legislation applicable to the processing of personal data by the Customer or Wintro within the scope of the Agreement, such as, but not limited to: **(i)** the General Data Protection Regulation 2016/679 of April 27, 2016 ("**GDPR**"); **(ii)** the Belgian Privacy Law of 30 July 2018; **(iii)** the ePrivacy Directive 2002/58/EC of 12 July 2002, including future amendments and revisions thereof; and/or **(iv)** (future) national legislation regarding the implementation of the GDPR;
Service:	the online service of Wintro, including the integrations, features and modules as set out in the Agreement, which can be accessed through the Wintro Platform;
Sub-processor	other third parties engaged by Wintro to process the Personal Data on behalf of the Customer and in accordance with the Customer's instructions, as identified in **Annex III**;
Website:	the Wintro website, namely: https://www.wintro.ai/, including any and all its subdomains) and its application domain https://www.wintro.app/.
Wintro Platform:	the Wintro platform as described and represented on the Website and as provided in accordance with the Agreement;
Wintro:	Wintro NV, a private limited company with registered office at Belfortstraat 24D, 9000 Gent, registered with the Crossroad Database for Enterprises under number 0804.199.680;

1.2 The (uncapitalized) terms "controller"; "personal data breach"; "process"; "processing"; "processor" shall have the meaning attributed to them in the Privacy Legislation.

2 ROLE OF THE PARTIES

2.1 The parties acknowledge that with regard to the processing of Personal Data under the Agreement:

2.1.1 For Personal Data obtained from publicly available internet sources (such as LinkedIn profiles), Wintro shall be considered the 'controller' in accordance with the Privacy Legislation;

2.1.2 For all other Personal Data processed under the Agreement, the Customer shall be considered the 'controller' and Wintro 'processor' in accordance with the Privacy Legislation. Further, Wintro may engage (a) Sub-processor(s) pursuant to the provisions of **Section 7**.

2.2 Each party shall comply with its respective obligations under the Privacy Legislation with respect to the processing of the Personal Data.

3 SUBJECT MATTER

3.1 The Customer acknowledges that by making use of the Wintro Platform and/or Service, pursuant to the Agreement, it may provide (certain sets of) the Personal Data to Wintro for processing. Wintro shall also process Personal Data obtained from different, publicly available, internet sources for the execution of the Agreement. The nature and purpose of said processing, as well as a description of the Personal Data and categories of Data Subjects processed under the Agreement are further specified in **Annex I**.

3.2 Wintro shall process the Personal Data in a proper and careful way and in accordance with the Customer's instructions, the Privacy Legislation and other applicable rules/best-practices concerning the processing of personal data.

3.3 More specifically, Wintro shall

- ❑ during the performance of the Service, provide all its know-how in order to perform the Agreement according to the rules of art, as it fits a specialized and 'good' data processor; and,
- ❑ shall adopt, to the best of its abilities, the necessary security measures (cfr. **Annex II**) and provide all its know-how in order to perform the Service in accordance with the rules of art.

3.4 The Customer keeps full control concerning the following: (i) how the Personal Data must be processed by Wintro; (ii) the types of Personal Data processed; (iii) the categories of Data Subjects whose Personal Data is subjected to the processing; (iv) the purpose of the processing; and (v) the fact whether such processing is proportionate.

4 INSTRUCTIONS FROM / RESPONSIBILITY OF THE CUSTOMER

4.1 **Instructions**. Wintro shall only process the Personal Data upon the Customer's request and in accordance with the Customer's lawful instructions in **Annex I**, unless any legal obligation states otherwise. Wintro shall inform the Customer, if in its opinion, the instructions infringe the Privacy Legislation. If the Customer subsequently cannot guarantee the validity or legality of the instruction or fails or refuses to change the unlawful instruction so that it no longer violates the Privacy Legislation, Wintro shall be entitled to (i) suspend/refuse the performance of said instruction and (ii) at its discretion, to either continue to process the Personal Data in accordance with previously provided instructions or to stop the processing altogether, until the Customer has revised its instruction so that it no longer violates the Privacy Legislation .

4.2 **Responsibilities**. Furthermore, the Customer acknowledges that it is responsible for:

- ❑ the accuracy, quality and legality of (the collection and transfer of) the Personal Data;
- ❑ compliance with all transparency and lawfulness requirements under the Privacy Legislation for the collection and processing of the Personal Data and the transfer thereof to Wintro;
- ❑ processing Personal Data on the basis of the correct legal grounds;
- ❑ fulfilling its transparency obligations in accordance with the Privacy Legislation; and,
- ❑ ensuring compliance of its instructions (cfr. **Annex I**) with the Privacy Legislation.

4.3 Customer shall inform Wintro without undue delay if it is not able to comply with its responsibilities under this Section or the Privacy Legislation.

5 USE OF THE WINTRO PLATFORM AND THE SERVICE

5.1 In relation to (the processing of) the Personal Data, the Customer recognizes that:

- ❑ Wintro acts as a facilitator of the Service and the Wintro Platform. Therefore, the Customer shall be responsible on how and to what extent it makes use thereof;
- ❑ it is responsible for all acts and omissions of Authorized Users (i.e. in case the Authorized User does (not) take sufficient measures to protect its account on the Wintro Platform);

- ❑ Wintro allows the Customer to make adjustments and/or changes to the Personal Data and shall never adjust such Personal Data for itself and/or process the personal data for its own purposes, unless the Customer requests Wintro to do so;
- ❑ it is responsible for the material and/or data (including Personal Data) provided (directly and/or indirectly) by the Data Subject. The Customer is, as controller, thus responsible for complying with the Privacy Legislation and/or any other regulations with regard to aforementioned material and/or data;
- ❑ it shall comply with all laws and regulations (such as, but not limited to: with regard to the retention period or rights of the Data Subject) imposed on it by making use of the Service.

5.2 In case of any misuse of the Service or the Wintro Platform by the Customer or its Authorized Users in relation to the Personal Data and/or under this DPP or the Privacy Legislation, Wintro can never be held liable in this respect nor for any damage that would occur.

5.3 The Customer shall avoid any misuse of the Service and the Wintro Platform in relation to the Personal Data and/or under this DPP or the Privacy Legislation. Therefore, the Customer shall safeguard Wintro when such misuse would occur as well as for any claim from a Data Subject and/or third party due to such misuse.

6 SECURITY

6.1 Wintro takes the security of the processing activities very seriously. Wintro implements appropriate technical and organizational measures, as set forth in **Annex II**, to ensure, to the best of its abilities, the protection of (i) the Personal Data – including protection against careless, improper, unauthorized or unlawful use and/or processing and against accidental loss, destruction or damage; and (ii) the confidentiality and integrity of the Personal Data. When implementing said measures, Wintro has taken into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

7 SUB-PROCESSORS

7.1 Approval of Sub-processors

7.1.1 The Customer acknowledges and agrees that Wintro may engage Sub-processors in connection with provision of the Service (and the performance of the Agreement). In such a case, Wintro shall ensure that the Sub-processors are at least bound by the same obligations by which Wintro is bound under this DPP.

7.1.2 Wintro has currently appointed as Sub-processors as listed in **Annex III**.

7.1.3 Wintro shall be liable for the acts and omissions of its Sub-processors to the same extent as if it would be performing the Service/processing of the Personal Data itself, directly under the terms of this DPP.

7.2 Update of Sub-processor list

7.2.1 Wintro shall:

- ❑ update the list whenever a Sub-processor changes (e.g. a new Sub-processor was added, a Sub-processor was substituted, etc.);
- ❑ clearly indicate the changes in the list; and,
- ❑ add a timestamp (i) when the list was updated, and (ii) when the change of the Sub-processor went or will go into effect.

7.2.2 Wintro shall notify the Customer (e.g. on the Website or through the Wintro Platform) when changes to the list are made.

7.3 Objection

7.3.1 If the Customer wishes to exercise its right to object to a new Sub-processor, it shall notify Wintro in writing (cfr. **Section 15**) and based on reasonable grounds by the latest within thirty (30) days after the notification. If the Customer does not object or fails to object within the aforementioned timeframe it shall be deemed to have waived its right to object and to have authorized Wintro to engage the new Sub-processor.

7.3.2 In the event the objection is valid and reasonable grounds are formulated clearly, parties will discuss the Customer's concerns with a view to achieving a reasonable solution. Such solution may include, at Wintro's discretion, to (i) make available to the Customer a change in the Service; or (ii) recommend a commercially reasonable change to the Customer's use of the Service to avoid the processing of the Personal Data by the objected new Sub-processor without unreasonably burdening the Customer.

7.3.3 If the parties are, however, unable to come to a solution within a reasonable period of time (which shall not exceed thirty (30) days following the objection of the Customer), the Customer may terminate the Service (in whole or partly) if:

- ❑ the Service/Wintro Platform cannot be used by the Customer without appealing to the objected new Sub-processor; or,
- ❑ such termination solely concerns that part of the Service which cannot be provided by Wintro without appealing to the objected new Sub-processor;

and this by providing written notice thereof to Wintro (cfr. **Section 15**) within a reasonable time.

7.3.4 Termination of the Service within the meaning of **Section 7.3.3** shall be without liability to either party (but without prejudice to any fees incurred by the Customer prior to suspension or termination of the Service).

8 TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

8.1 The Personal Data shall in principle mainly be processed within the European Economic Area ("**EEA**").

8.2 However, the Customer recognizes that Wintro is entitled to transfer and store the Personal Data to countries outside the EEA for the purpose of providing the Service and fulfilling its obligations under the Agreement, and provided that such transfer/storage is done in accordance with the Privacy Legislation regarding additional safeguards. In particular, any transfer of Personal Data outside the EEA by Wintro to a third party whose domicile or registered office is in a country which does not fall under an adequacy decision enacted by the European Commission, shall be additionally subject to one or more of the listed EU-approved safeguards:

- ❑ ***European Commission Adequacy decision***
- ❑ ***closing a data transfer agreement****:* with the third country recipient, which shall contain the standard contractual clauses, as referred to in the 'European Commission implementing decision of 4 June 2021 (**Decision (EU) 2021/914**) on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council', including the performance of a transfer impact assessment. Before the transfer takes place, the recipient of the Personal Data/Sub-processor of Wintro in the third country has to guarantee Wintro that an adequate level of privacy compliance is ensured in this third party country;
- ❑ ***binding corporate rules***: As it is the case for standard contractual clauses, the recipient of Personal Data/Sub-processor of Wintro in the third country has to guarantee Wintro that an adequate level of privacy compliance is ensured in the third party country; and/or,
- ❑ ***certification mechanisms***.

8.3 In the event the transfer (or disclosure) of the Personal Data to a third country is required by EU law or EU member state law to which Wintro is subject to, Wintro shall inform the Customer of that legal requirement before the transfer/disclosure, unless that law prohibits such information on important grounds of public interest.

9 CONFIDENTIALITY

9.1 Wintro shall maintain the Personal Data confidential and thus not disclose nor transfer the Personal Data to third parties, without the Customer's permission, unless when such disclosure and/or transfer is required by law or by a court or other government decision (of any kind). In such case Wintro shall, prior to any disclosure and/or announcement, inform the Customer in full transparency on the scope and manner thereof.

9.2 Wintro ensures the Customer that individuals engaged in the performance of the Service (such as, personnel, representatives, officers, directors, agents, advisors, affiliates and consultants) are (i) informed of the confidential nature of the Personal Data; (ii) are well aware of their responsibilities; and (iii) are bound by written confidentiality agreements. Wintro ensures that such confidentiality obligations survive the termination of their employment or service contract.

9.3 Wintro ensures the Customer that the access of its personnel to the Personal Data is limited to such personnel performing the Service in accordance with this DPP.

10 NOTIFICATION OBLIGATIONS AND ASSISTANCE

10.1 Notification. Wintro shall use its best efforts to inform the Customer as soon as reasonably possible when it:

- ❑ receives a request for information, a subpoena or a request for inspection or audit from a competent public authority (incl. supervisory authority) in relation to the processing of the Personal Data;

- ❑ receives a request from a Data Subject invoking its privacy rights under the Privacy Legislation (cfr. **Section 10.3**);
- ❑ has the intention to disclose Personal Data to a competent public authority (incl. supervisory authority); or,
- ❑ determines or reasonably suspects a personal data breach has occurred in relation to the Personal Data.

10.2 Personal data breach. In case of a personal data breach, Wintro:

- ❑ shall notify the Customer without undue delay after becoming aware of this personal data breach and, to the extent possible, provide the information as required by Privacy Legislation (e.g. Article 33.3 GDPR). Upon request of the Customer, Wintro shall provide – to the extent possible – assistance with respect to the Customer's reporting obligation under the Privacy Legislation;
- ❑ undertakes – as soon as reasonably possible – to take appropriate remedial actions to make an end to the personal data breach (if such has occurred under its responsibility) and to prevent and/or limit any future personal data breaches.

10.3 Rights of Data Subjects

10.3.1 Wintro shall promptly notify the Customer if it receives a request from a Data Subject invoking its privacy rights under the Privacy Legislation. Wintro shall not respond to any such Data Subject request without the Customer's prior written consent, except to confirm that the request relates to the Customer to which the Customer hereby agrees.

10.3.2 If a Data Subject requests to exercise his/her/their rights, it is the Customer's responsibility to assist the Data Subject in its request. Only if the Customer does not have the ability to correct, amend, block or delete the Personal Data (as required by Privacy Legislation), Wintro shall assist the Customer (as long as commercially reasonable).

10.3.3 Notwithstanding the foregoing, the Customer remains responsible for compliance of such Data Subject requests.

10.4 Data Protection Impact Assessment. Taking into account the nature of the processing and to the extent that (i) the Customer is required to perform a data protection impact assessment under the Privacy Legislation as a consequence of the Agreement and (ii) the required information is reasonable available to Wintro and the Customer does not otherwise have access to said information, Wintro shall – upon request of the Customer – provide reasonable assistance to the Customer with the execution of a data protection impact assessment and possible prior consultation with the competent supervisory authorities. To the extent permitted by the Privacy Legislation, the Customer shall be responsible for any costs arising from Wintro's provisions of such assistance.

11 LIABILITY

11.1 Both parties are solely liable for all damage, claims and/or fines of third parties, competent supervisory authorities or Data Subjects that are the result of their own breach of or non-compliance with (i) the provisions of this DPP, and (ii) the Privacy Legislation or other applicable rules concerning Personal Data. Each party shall indemnify the other party in this regard.

11.2 In case of breach/non-compliance as described in **Section 9.1** the infringing party is liable to the other party and must reimburse the latter for all damages and costs, including reasonable attorney's fees, (legal) expenses and damage resulting from such a breach/non-compliance.

11.3 In case of a proven breach by Wintro of its obligations under this DPP or under the Privacy Legislation, Wintro shall:

- ❑ be liable for the proven direct damages incurred by the Customer;
- ❑ **not** be liable for indirect, immaterial and/or consequential damages, including (but not limited to:) loss of profit, loss of opportunities, loss of and/or damage to data, loss of reputation, sanctions and/or fines, and unforeseeable damages.

11.4 Wintro's liability towards the Customer shall in any case be limited to the total amount paid by the Customer to Wintro during the last twelve (12) months under the Agreement.

11.5 The provisions in this Section shall be without prejudice to any other liabilities and limitations of liabilities as agreed upon in the Agreement.

12 TERM

12.1 The total term of this DPP shall be the term of the Agreement. If no term is determined, this DPP shall remain in force as long as the Service has not come to an end.

13 RETENTION, RETURN AND DELETION OF PERSONAL DATA

13.1 Wintro shall only retain the Personal Data as long as needed to provide the Service or for the term of the Agreement (cfr. **Section 12**). The Customer accepts that Wintro may create back-ups of the Personal Data stored on the Wintro Platform.

13.2 Upon termination of the Service or the Agreement, the following shall apply:

- ❑ the Service and Wintro Platform shall be deactivated. Any Personal Data, stored on the Wintro Platform shall as from that moment no longer be available to the Customer;
- ❑ the Customer may request the Personal Data to be returned ('export') within ninety (90) days following the end of the Agreement or the Service, upon which Wintro shall assess whether such export is possible from a technical perspective. In any event, Wintro may, at its sole discretion, determine the format of the export. Wintro reserves the right to charge any costs relating to such exports to the Customer.
- ❑ after said ninety (90) days-period, the Personal Data on the Wintro Platform shall be deleted within one (1) month, unless it is required by applicable law to retain the Personal Data.
- ❑ the Personal Data may be present on back-ups. The Personal Data shall be deleted once the last back-up containing the Personal Data is rotated.

13.3 Please note that data or material provided to or submitted to Wintro by the Customer during the use of the Service that does not contain Personal Data may be further stored by Wintro following the termination of the Agreement or the Service.

14 COMPLIANCE / INSPECTIONS

14.1 Compliance. Upon the Customer's request, Wintro shall make available to the Customer all information necessary and to the extent as requested by law to demonstrate its compliance with its obligations under this DPP.

14.2 Inspections

14.2.1 Wintro shall allow the Customer (or a third party on its behalf) to carry out inspections – such as, but not limited to: an audit – and shall provide the necessary assistance thereto.

14.2.2 However, the Customer shall limit its initiatives to perform an inspection to a maximum of once a year. The Customer must notify Wintro at least thirty (30) working days in advance. The performance of inspections may in any case not cause any delay in the performance of the Service by Wintro.

14.2.3 Wintro can in any case refuse any inspection if the subject of the inspection was already certified by a renown certifying organization.

14.2.4 The Customer shall impose sufficient confidentiality obligations on its (internal/external) auditors. As to ensure the confidentiality of other Wintro customers, Wintro has the right to require from the Customer and its auditors to sign a non-disclosure agreement before the start of the inspection and to limit the scope of the inspection or the access of the Customers to certain premises.

14.2.5 All inspection costs are exclusively borne by the Customer, except if (and to the extent that) a severe security incident/personal data breach (at Wintro/under Wintro's responsibility) or a violation of this DPP is determined during the inspection.

15 NOTIFICATION / CONTACT WINTRO

15.1 Notifications by the Customer under this DPP and/or any questions or concerns with regard to the provisions of this DPP must be directed at privacy@wintro.ai.

16 GOVERNING LAW & JURISDICTION

16.1 This DPP, including its Annexes, shall be governed by the law and subject to the jurisdiction clause as provided in the Agreement.

Annex I – Data Processing

1 OVERVIEW OF THE PERSONAL DATA

Data Subjects – Category 1

- ❑ Name
- ❑ First name
- ❑ LinkedIn profile
- ❑ LinkedIn network
- ❑ Company
- ❑ Company e-mail address
- ❑ Personal e-mail address
- ❑ LinkedIn cookies

Data Subjects – Category 2

- ❑ Name
- ❑ First name
- ❑ LinkedIn profile
- ❑ Company
- ❑ Company e-mail address
- ❑ LinkedIn network

Data Subjects – Category 3

- ❑ Name
- ❑ First name
- ❑ LinkedIn profile

2 OVERVIEW OF THE DATA SUBJECTS

Category 1

- ❑ Authorized User
- ❑ Recruiter Customer

Category 2

- ❑ Employee Customer
- ❑ Directors of Customer

Category 3

- ❑ LinkedIn users in employees' connected network

3 NATURE OF THE PROCESSING

- ❑ Collecting
- ❑ Sorting
- ❑ Structuring
- ❑ Modifying
- ❑ Saving
- ❑ Transferring
- ❑ Consulting
- ❑ Comparing
- ❑ Interconnecting
- ❑ Communicating
- ❑ Matching
- ❑ Deleting

4 MEANS OF PROCESSING

- ❑ Through the Wintro Platform
- ❑ Artificial Intelligence

5 PURPOSE OF THE PROCESSING

Providing the Service and access to/use of the Wintro Platform pursuant to the Agreement.

6 DURATION

For the term of the Agreement (cfr. Wintro's Terms of Use applicable to the Customer). Upon termination of the Agreement (for whatsoever reason), access to the Wintro Platform shall be deactivated and the Personal Data shall either be deleted or returned to the Customer as provided in **Section 13**.

Annex II – Security

1. MANAGEMENT INFORMATION SECURITY

(i) Wintro has implemented an appropriate information security policy.

(ii) Wintro has suitably qualified information security specialists, supported by the Wintro leadership.

(iii) Wintro management requires employees and third-party contractors with access to Customer information to commit to written, confidentiality, and privacy responsibilities with respect to that information. These responsibilities survive termination or change of employment or engagement.

(iv) Wintro management provides information security awareness information to employees and relevant third-party contractors.

2. ACCESS CONTROL

2.1. User Access Management

(i) Wintro implements access control policies to support creation, amendment and deletion of user accounts for systems or applications holding or allowing access to Customer information.

(ii) Wintro implements a user account and access provisioning process to assign and revoke access rights to systems and applications.

(iii) The use of “generic” or “shared” accounts is prohibited without system controls enabled to track specific user access and prevent shared passwords.

(iv) Wintro monitors and restricts access to utilities capable of overriding system or application security controls.

(v) User access to systems and applications storing or allowing access to Customer information is controlled by a secure logon procedure.

2.2. Physical Access Management

(i) Physical access to facilities where Customer information is stored or processed is protected in accordance with good industry practices.

(ii) Physical documents shall always be kept in a secluded spaces to which access shall only be granted on a need-to-know basis.

3. COMMUNICATIONS AND CLOUD SECURITY

(i) Wintro logically segregates Customer data within a shared service environment.

(ii) Wintro secures network segments from external entry points where Customer data is accessible.

(iii) External network perimeters are hardened and configured to prevent unauthorized traffic.

(iv) Inbound and outbound points are protected by firewalls and intrusion detection systems (IDS). c. Ports and protocols are limited to those with specific business purposes.

(v) Wintro synchronizes system clocks on network servers to a universal time source (e.g. UTC) or network time protocol (NTP).

(vi) Customer data, including Personal Data, is encrypted at rest.

(vii) Wintro encrypts data during transmission between each application tier and between interfacing applications.

4. OPERATIONS SECURITY

4.1. Service Management

(i) Wintro has implemented formal operating procedures for system processes impacting Customer data. This notification may occur through generic change logs. Procedures must track author, revision date and version number, and must be approved by management.

(ii) Wintro monitors service availability.

4.2. Vulnerability Management

(i) Wintro performs annual penetration testing for systems and applications that store or allow access to Customer data, including Personal Data. Identified issues must be remediated within a reasonable timeframe.

(ii) Wintro has implemented a patch and vulnerability management process to identify, report and remediate vulnerabilities by:

- ❑ implementing vendor patches or fixes; and,
- ❑ developing a remediation plan for critical vulnerabilities.

(iii) Wintro has implemented controls to detect and prevent malware, malicious code and unauthorized execution of code. Controls must be updated regularly with the latest technology available (e.g. deploying the latest signatures and definitions).

4.3. Logging and Monitoring

(i) Wintro generates administrator and event logs for systems and applications that store or allow access to Customer data.

(ii) Wintro reviews system logs periodically to identify system failures, faults, or potential security incidents affecting Customer information.

5. RESILIENCE

(i) Wintro performs business continuity risk assessment activities to determine relevant risks, threats, impacts, likelihood, and required controls and procedures.

(ii) Based on risk assessment results, Wintro documents, implements, annually tests and reviews its Business Continuity and Disaster Recovery (BC/DR) plans to validate the ability to restore availability and access to Customer data in a timely manner, in the event of a physical or technical incident that results in loss or corruption of Customer data.

6. THIRD-PARTY SUPPLIER MANAGEMENT

(i) Wintro has contractual agreements with third parties handling Customer information which must include appropriate information security, confidentiality, and data protection requirements, as detailed in the Agreement. Agreements with such parties are reviewed periodically to validate that information security and data protection requirements remain appropriate.

(ii) Wintro reviews its third parties' information security controls periodically and validates that these controls remain appropriate according to the risks represented by the third party's handling of Customer information, taking into account any state-of-the-art technology and the costs of implementation.

(iii) If requested by Customer, Wintro provides the Customer a list of third parties with required access to Customer data, including Personal Data.

(iv) Wintro restricts access to personal data but may permit access to Customer data, including Personal Data, only as necessary to perform the services that the third party has contractually agreed to deliver.

7. AUDIT AND COMPLIANCE

(i) Wintro periodically reviews whether its systems and equipment storing or enabling access to Customer data, including Personal Data, comply with legal and regulatory requirements and contractual obligations owed to Customer.

(ii) Wintro maintains current independent verification of the effectiveness of its technical and organizational security measures (e.g. ISO certification). The independent information security review are performed at least annually.

Annex III – Sub-processors

Last updated: May 2024

Wintro engages the following Sub-processors to assist in providing the Service as described in the Agreement:

1. SUBPROCESSORS

Name	Nature of processing	Territory
Google Cloud Platform	Cloud Service Provider	EEA
Amazon Web Services Inc.	Cloud Service Provider	EEA
Microsoft Azure	Azure OpenAI/GPT API	EEA
Vercel	Web application hosting	EEA
Supabase	Cloud database hosting & Authentication	EEA
iScraper	Fetching of public LinkedIn data	EEA
PhantomBuster	Automation of social media interactions	EEA
Kombo	ATS synchronization	EEA