PRIVACY AND PERSONAL DATA PROTECTION POLICY

Approved by the Data Protection Officer

---

1. General Purpose

This Policy is intended to inform you of the practices of Dipôle Solutions inc. (hereinafter 'Dipôle') and our subsidiaries and affiliated companies (including, without limitation, 'Cognito App™', 'Cognito™', 'Cognito Coach™' and 'Cognito-app™') regarding the governance and confidentiality of its customers' personal data (hereinafter the 'Data'). It applies to all Users and all our services, including our websites (collectively, the 'Websites'), our web applications ('Web Applications'), our mobile applications ('Mobile Applications') and all associated services (collectively, the 'Services').

It is also intended to ensure the security and protection of Data collected, processed, used, disclosed and retained by Dipôle against unauthorized access, use or disclosure. It also aims to protect such Data against any impairment of its integrity.

Furthermore, this Policy establishes the rules governing the processing of such Data, including access, disclosure, use, retention and destruction, as well as rights of access, portability, rectification, withdrawal, erasure and objection, as applicable.

2. Legal Basis

Dipôle is a private-sector company subject, in particular, to the Act respecting the protection of personal information in the private sector (CQLR, c. P-39.1), the Act to establish a legal framework for information technology (CQLR, c. C-1.1), the Civil Code of Québec (CQLR, 1991, c. 64), the Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), and the European Union General Data Protection Regulation (hereinafter the 'GDPR').

3. Applicable Laws

Data processing practices may vary depending on the jurisdictions in which Dipôle operates.

Considering that all of Dipôle's customers are businesses, this Policy draws more heavily on the GDPR. However, should an individual residing in Québec become a customer of Dipôle, this Policy shall also apply in Québec.

This Policy applies to all Website users, regardless of their location.

Dipôle recognizes the importance of privacy, security and Data protection. It therefore undertakes to comply with the provisions, values and fundamental principles established by all applicable legislation, including any updates thereto.

Dipôle ensures that the necessary physical, computer and technological security measures are implemented to preserve the confidentiality of Data communicated to it in the course of its activities.

4. Scope of Application

This Policy applies to all employees, agents, suppliers and partners of Dipôle who may have access to Data in the performance of their duties.

This Policy concerns the Data of Dipôle's customers and Website users. Dipôle's customer and Website user are hereinafter referred to as the 'Customer'.

5. Objectives

This Policy seeks to define the types of Data collected by Dipôle and the means by which Dipôle protects such Data.

It also specifies standards governing the collection, use, disclosure, retention and destruction of such Data, as well as rights of access, portability, rectification, withdrawal, erasure and objection, as applicable, concerning Data held by the company or a third party, regardless of the medium on which they are recorded or the form in which they are available: written, graphic, audio, visual, computerized or otherwise.

6. Definition of Data

Any factual or subjective information relating to a natural person that makes it possible to identify that person, directly or indirectly, and that is not public under the law.

Applicable in Québec: However, Data does not include business contact information, such as a name and job title, as well as a workplace postal address, email address and telephone number, where such information is used to communicate with an individual in the course of their professional duties.

7. General Principles

Dipôle takes security measures appropriate to protect Data that are collected, processed, used, disclosed, retained or destroyed, and that are reasonable in light of, in particular, their sensitivity, the purpose of their use, their quantity, distribution and medium, including by ensuring the following:

- The integrity of Data, so that they are not destroyed or altered in any way without authorization and in accordance with applicable laws, and so that their medium provides the required stability and durability;
- The confidentiality of Data, by limiting their disclosure to persons authorized to access them;
- Identification and authentication, so as to confirm, when required, a person's identity or the identification of a document or device;
- Compliance with the legal, regulatory or business requirements to which Dipôle is subject.

8. Collection of Data

Dipôle is a professional software development company. In the course of its activities, Dipôle collects Data about its Customers directly from them or from third parties. Where applicable, Dipôle informs its Customers of Data collected from such third parties. In all cases, it informs the Customer of the purposes for which the Data are processed, the categories of persons within the company who have access to the Data, the retention period and the contact details of the person responsible for Data processing. This information is provided within a reasonable time after obtaining the Data, but no later than one (1) month, taking into account the particular circumstances in which the Data are processed. However, if the Data are processed for the purpose of communicating with the Customer, this information is provided no later than the first communication with the Customer. Likewise, if disclosure of the Data to another recipient is contemplated, this information is provided no later than the first such disclosure.

Dipôle may collect, in particular, the following Data:

- Contact details, such as first and last name, postal address, email address, IP address and telephone number;
- Billing information, such as a billing address, banking information, credit card details or payment-system information;
- Documents, notes, forms, audio or video recordings, transcripts and reports generated with the assistance of artificial intelligence.
- Data relating to the use of Dipôle's Services, including technical data concerning visits or any other Data collected through cookies;
- Any other Data requested and provided in connection with the Services offered.

The extent of the Data collected depends on Customers' interactions with Dipôle and their use of its Services.

9. Sensitive Data

Dipôle does not knowingly collect sensitive personal Data, such as health information, information on ethnic origin or biometric Data.

10. Consent to Collection

Dipôle collects Data transparently and with the Customer's prior, free and informed consent, obtained through one or more consent forms explained in simple and clear terms or through a pop-up window upon arrival on the Website.

In accordance with applicable laws, when Dipôle collects Data, it requests the Customer's consent by informing them in advance of the purposes for which the Data are collected and will be used.

Dipôle will obtain new and separate consent before using Data in its possession for purposes incompatible with those for which they were initially collected, and will inform the Customer of the significance and anticipated consequences of such processing for them.

11. Methods of Collection

Data may be collected directly by Dipôle or by a third party, including in person, by email, through forms, telephone interviews, questionnaires, social media, text messages, or electronically through Dipôle's Website or an application.

Dipôle collects Data from the Customer with their prior consent and provides, at the time of collection and thereafter upon request, the following information, in particular, in simple and clear terms:

- Dipôle's name;
- The purposes for which the Data are collected;
- The means by which the Data are collected;
- The rights of access, portability, rectification, withdrawal, erasure and objection, as applicable, provided under applicable laws;
- The name of the third party on whose behalf the collection is carried out, where applicable;
- The names of third parties to whom the Data must be disclosed;
- The possibility that Data may be disclosed outside Québec or outside the European Union, as applicable.

Upon request, Dipôle will inform the Customer of the Data collected from them, the categories of persons within the company who have access to such Data, the Data retention period, and the contact details of the Data Protection Officer.

12. Use

Dipôle collects, uses and retains Customer Data in particular to:

- Verify their identity;
- Communicate with them;

- Personalize its Services;
- Provide a quotation;
- Send notifications and newsletters;
- Provide customer service;
- Improve the Services offered;
- Offer personalized Services;
- Provide assistance and resolve technical issues;
- Generate invoices, account statements and reports;
- Manage different Customer accounts;
- Generate reports containing statistical Data;
- Generate, at the professional's request, transcripts and AI-assisted meeting reports.
- Share Data with third parties for storage purposes;
- Improve, personalize and develop its Website;
- Provide customer service on its Website;
- Provide updates and other information concerning its Website;
- Conduct marketing and promotional activities;
- Perform profiling;
- As permitted or required by any applicable legal or regulatory obligation or provision;
- Any other compatible purpose;
- Enforce its rights, where applicable.

Dipôle uses collected Data solely for the purposes for which consent was obtained. Accordingly, unless specific consent has been given, Dipôle does not disclose, sell, rent, give, exchange, share or otherwise communicate any Data to any third party.

Such Data are accessible only to Dipôle's employees, suppliers or agents who necessarily require them to perform their duties, and these persons are required to maintain the confidentiality of the Data.

13. Data Retention and Security

All Data collected, regardless of their medium, are retained in a secure environment protected against unauthorized access, disclosure, copying, use, alteration or destruction, as well as loss or theft.

These security measures include, where applicable, firewalls and secure servers, encryption, the implementation of appropriate access-rights management systems and procedures, careful selection of processors, adequate training of Dipôle personnel who have access to Data in the course of their duties, and other measures necessary to protect Data appropriately against unauthorized use or disclosure. Dipôle uses information technology to support its business processes so as to provide better Services and appropriate security for the Data it holds.

Dipôle implements appropriate security and access-management measures to ensure the confidentiality, integrity and availability of the Data it holds, in light of their sensitivity, the risks to which they are exposed and the obligations to which Dipôle is subject.

14. Disclosure of Data to Third Parties

Dipôle requires the Customer's consent before disclosing Data concerning the Customer to a third party, unless applicable laws authorize disclosure without such consent.

In the course of providing its Services, Dipôle may, in accordance with applicable legal requirements, disclose Data to third parties located in Québec, outside Québec or outside the European Union, as applicable. Such third parties include government authorities, financial institutions and information technology service providers. In such cases, Dipôle's external service providers are subject to confidentiality agreements and legal restrictions prohibiting the use of disclosed Data for purposes other than those for which Dipôle collected them. Dipôle may also enter into service agreements with its external providers, in compliance with the law, to facilitate the sharing of Data among them and with other stakeholders.

When Data are disclosed to third parties outside Québec or outside the European Union, Dipôle conducts a privacy impact assessment. In doing so, Dipôle takes account of the sensitivity of the Data and the nature, scope, context and purposes of the proposed processing. Data may be disclosed outside the European Union when appropriate safeguards are provided for the intended purpose, such as standard data-protection clauses approved by the European Commission on the advice of the European Data Protection Board, unless those bodies have determined that the country provides an adequate level of protection. Data may be transferred outside Québec when appropriate contractual safeguards are established for the intended purpose.

Dipôle and its suppliers may be required to provide retained Data pursuant to a court order, an administrative investigation or another situation provided for by law.

In connection with a sale, buyout, acquisition or any other restructuring of Dipôle's business, Dipôle may be required to disclose Data to potential or existing purchasers and their advisers for the purposes of the transaction. Dipôle will ensure compliance with applicable legal requirements before any disclosure.

15. Customer Rights

The rights identified below may be exercised by contacting the Data Protection Officer identified in section 26 of this Policy.

a) Right of Access and Right to Data Portability

The Customer has the right to access Data concerning them that are held by Dipôle, subject to exceptions under applicable laws.

Applicable in Québec: Unless this raises serious practical difficulties, computerized Data collected directly or indirectly from the Customer will be provided in a structured, commonly used technological format.

Applicable only under the GDPR: The Customer may request that their Data be returned to them or transferred to another company in certain circumstances and subject to applicable legal requirements. Such Data must be provided in a commonly used, machine-readable format.

b) Right to Rectification

The Customer may request that their Data be corrected, rectified or updated.

c) Right of Withdrawal and Right to Erasure (Right to Be Forgotten)

The Customer may request that their Data be destroyed or no longer used for the purposes for which they were collected.

The Customer may also withdraw consent to the use of their Data at any time. Such withdrawal shall have prospective effect only, upon receipt by Dipôle. Upon receiving notice of withdrawal of consent, Dipôle undertakes to cease all use of the Data concerned and to destroy them, subject to any statutory or regulatory retention obligation.

However, Dipôle may be unable to fulfil its obligations in the event of a request to withdraw consent or for early destruction. In such cases, Dipôle shall not be liable for any harm suffered by the Customer.

Dipôle will also notify any person or entity to whom such Data have been disclosed in accordance with the consent obtained, so that they may also cease using and destroy such Data, as applicable.

d) Right to Object

Applicable only under the GDPR: The Customer may object to the processing of their Data for a particular use.

16. Destruction

Data are retained for the period necessary to fulfil the purposes for which they were collected and are subsequently destroyed. Data may be retained beyond fulfilment of those purposes where another statutory retention period applies. They will be destroyed in accordance with applicable

laws or, where applicable, processed so that they can no longer be attributed to the Customer, for example through anonymization.

17. Customer Responsibility

The Customer who sends Data to Dipôle is responsible for their accuracy.

Any Customer who sends Data to Dipôle must also ensure that the system or equipment used to send or receive information from Dipôle is sufficiently secure and must exercise vigilance. Dipôle shall not be liable for unauthorized access to Data resulting from negligence or vulnerabilities in a Customer's equipment or system.

If the confidentiality of their Data is compromised or their identity is stolen, the Customer must notify Dipôle as soon as possible by contacting the Data Protection Officer identified below.

18. Data Breaches and Measures to Be Taken

A Data breach includes unauthorized access to Data under the law, unauthorized use or disclosure of Data under the law, loss of Data or any other breach of their protection. In the event of a Data breach, Dipôle will promptly take the measures required to reduce the risk of harm to the Customer and prevent further breaches of the same nature.

Applicable in Québec: Where there is a risk of serious injury, Dipôle will notify the Customer and the Commission d'accès à l'information.

Applicable under the GDPR: Where the breach creates a risk to the Customer's rights and freedoms, Dipôle will notify the Data Protection Authority without undue delay and, where feasible, no later than 72 hours after becoming aware of it. In addition, where the breach creates a high risk to the Customer's rights and freedoms, Dipôle will inform the Customer as well as the Data Protection Authority.

19. Obligations in the Event of Access to a Third Party's Data

Any person who has accessed Data not concerning them, for whatever reason, must maintain their confidentiality. They are strictly prohibited from disclosing, using, distributing or reproducing such Data. They must also immediately inform the Data Protection Officer identified below and securely destroy the Data and all copies thereof in accordance with applicable laws.

20. Maintenance of a Data Breach Register

Dipôle maintains a register of all Data breaches it has experienced, where applicable, including those that do not present a risk of serious injury to the Customer.

Dipôle will make this register available for inspection by the Commission d'accès à l'information or the Data Protection Authority, as applicable, and may provide them with a copy upon request.

21. Cookies and Privacy Settings

To provide certain Services, Dipôle may also collect Data through its Website using the following technologies:

- Cookies: When a Customer visits its Website, the Website sends one or more cookies to the Customer's computer, along with cookies from related services such as Google Analytics, Google Adwords, Google Adsense or Facebook. These cookies contain identifying information enabling Dipôle to understand how Customers interact with the Services, target Customers with relevant offers, track their browsing history on the Website and summarize their experience of using the Services.

- Connection logs: Whenever a Customer accesses Dipôle's Services through its Website, the servers automatically record connection information sent by the Customer's browser when connecting to a website. Server connection logs may include information such as their Internet search, IP address, browser type and language, Internet service provider, connection date and time, pages visited, one or more cookies identifying the browser, and number of clicks.

Where required, information provided by a Customer during use may be combined with information from other Dipôle services or third parties such as Google Analytics, Google Adwords, Google Adsense or Facebook to improve the quality of the Services. For certain Services, the Customer may choose whether or not to allow such information to be combined.

If a Customer wishes to disable the advertising features of Google Analytics, Google Adwords, Google Adsense or Facebook, including through ad settings, mobile application ad settings or any other available means, they may consult the Internet to access the Google Analytics Opt-out Browser Add-on. Customers may also consult the following resources to learn more about third-party use of cookies and how to disable them: Google Advertising and Privacy, Google Ad Settings and the DAA page.

A consent banner is automatically displayed when the Customer arrives on the Website to allow them to enable cookies. The effectiveness of certain Website Services may be affected if the Customer declines to enable cookies. Cookies are divided into four (4) categories:

- Necessary cookies;

• Functionality cookies;
• Performance and security cookies;
• Tracking cookies.

Any Customer who provides Data under this section consents to their use and disclosure for the purposes for which they were collected.

22. Affiliated Websites

Some Dipôle Services may be offered in conjunction with other websites. Data that a Customer provides to such websites may be sent to Dipôle so that the Service can be provided. Such Data are processed in accordance with this Policy. Affiliated websites may have different privacy practices; Dipôle therefore recommends reviewing their applicable policies and practices.

23. Links

Dipôle may display links in a format that allows it to determine whether they have been followed. This information is used to improve the quality of content and personalized advertisements.

24. Complaint Management

Any Customer wishing to file a complaint regarding the collection, retention, use, disclosure or destruction of their Data by Dipôle, or rights of access, portability, rectification, withdrawal, erasure and objection, as applicable, must submit the complaint to Dipôle's Data Protection Officer. The Data Protection Officer will examine the complaint and provide a response within thirty (30) days of receipt.

25. Publication of this Policy

Dipôle publishes this Policy on its Website and disseminates it by any means appropriate to reach Customers. Dipôle does the same for the notice required for any amendment to this Policy.

26. Data Protection Officer

Mr. Dominic Crousset, President of Dipôle, is the Data Protection Officer. He may be reached by email at sécurité@dipolesoultions.ca, by telephone at 1-877-812-1580, extension 101, or in writing at 7380, boulevard Allard, Drummondville, Québec, Canada J2A 2S8.

The Data Protection Officer is a member of Dipôle's staff and has roles and responsibilities throughout the Data lifecycle within the company.

27. General Provision

This contract is written in French and may be translated into other languages for convenience. In the event of any discrepancy in interpretation between the French version and any translated version of this contract, the French version shall prevail.

28. Effective Date

This Policy shall enter into force on the date of its adoption by Dipôle's Board of Directors.

Approved by the Data Protection Officer 2026-11-07
