HAPPY SOUP LIMITED
(trading as dx0)

PRIVACY & COOKIES POLICY

(last updated on 11th August, 2026)

1. CONTACT DETAILS

We are **HappySoup Limited (trading as dx0)**, a company incorporated and registered in Ireland with company number 799682, whose registered office is at 17 Diswellstown Court, Hamilton Park, Castleknock, (referred to in this Privacy & Cookies Policy (the "**Policy**") as "**HappySoup**", "**we**", "**our**", or "**us**"). We are a software company based in Ireland (the "**Business**") providing tools for the Salesforce ecosystem. For privacy-related questions, contact us at help@happysoup.io.

2. SCOPE OF POLICY

This Policy applies to the dx0 product and our website dx0.io (the "**Website**") and AI agent agent.dxo.io and services related thereto (the "**Service**"). As our customer, your privacy is of paramount importance to us. This Policy is designed to protect you, our users, by informing you what Personal Data is collected, how we will use your Personal Data, with whom we share it, how long we keep it, your rights in respect of your Personal Data and how to contact us if you have any queries or concerns about our use of your Personal Data. Your use of the Website is subject to your agreement with this Policy.

In this Policy, the term "**Personal Data**" means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, our possession, and includes Personal Data as described in Data Protection Laws (as defined below).

We will handle your Personal Data in accordance with Data Protection Laws. "**Data Protection Laws**" means the Data Protection Acts 1988 to 2018, the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), and any other applicable law or regulation relating to the processing of Personal Data and to privacy, including the E-Privacy Directive 2002/58/EC and the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, as such legislation shall be supplemented, amended, revised or replaced from time to time and all guidance and codes of practice issued by a relevant supervisory authority, from time to time and which are applicable to us.

We are a controller (as defined in Data Protection Laws) in relation to any Personal Data which we collect from you through your or any other user's use of the Service and the set-up of Your account. This Policy sets out the basis on which any such Personal Data will be processed by us. You may be a data subject (as defined in Data Protection Laws) or you may be a controller. When you are a controller in respect of the Personal Data of other data subjects, then you must comply with all of your controller obligations under Data Protection Laws. When you are a controller, we and you act as independent controllers, unless agreed otherwise.

When a business customer connects a source system — such as Salesforce, or other platforms we may support from time to time — to dx0, our platform may access and process the metadata

and any Personal Data contained within that environment in order to deliver the Service. For example, if a financial institution uses Salesforce to manage their client relationships, that environment may contain Personal Data relating to both their own employees (such as system user names and email addresses) and their clients (such as contact names, email addresses, or other details stored within that system). When that institution connects the source system to dx0, this Personal Data may pass through our servers and, where AI-powered analysis is requested, may also be transmitted to our AI sub-processor, OpenAI, for processing.

In such cases, the business customer acts as the controller in respect of their employees' and clients' Personal Data, and we act as a processor on their behalf. The nature and extent of any Personal Data processed will depend entirely on the contents of the customer's connected source system(s) and how they choose to use the Service. We do not control, and take no responsibility for, the categories of Personal Data that customers elect to store within their connected source systems.

The extent of Personal Data we can access is determined by the permissions granted to the account used to connect the source system to dx0. We recommend customers use a dedicated integration account for this purpose, rather than a personal or administrator account, so that access can be scoped, audited, and revoked independently of any individual's credentials. Depending on the source system, customers may be able to further restrict access using that system's own permission sets, roles, or field-level security controls, limiting dx0 to the minimum data required for the features they intend to use. Where available, the specific permissions and scopes required by dx0 for each supported integration are documented on our Security Page.

For technical detail on how data is stored, encrypted, and protected, see our Security Page.

3. WHO THIS POLICY APPLIES TO

dx0 is a business-to-business (B2B) service. Our customers are companies and their authorised employees ("**users**"). This policy applies to all users of dx0, whether on a free trial or a paid plan and to any other individual who may provide us with Personal Data or who may provide Personal Data on behalf of another person from time to time.

4. PERSONAL DATA WE COLLECT

4.1 General

We fully respect your right to privacy in relation to your interactions with the Service and endeavour to be transparent in our dealings with you as to what Personal Data we will collect and how we will use your Personal Data. We only collect and use Personal Data where we are legally entitled to do so. Information in relation to Personal Data collected by Irish entities is available on the website of the Irish Data Protection Commission (**DPC**), https://www.dataprotection.ie.

We endeavour to keep your Personal Data accurate and up-to-date. As such, you must tell us about any changes to such information that you are aware of as soon as possible.

4.2 Account information

When you create a dx0 account, we collect your name, email address, and company name. If you authenticate via a connected source system (such as Salesforce OAuth), we additionally

receive identifying information from that system, such as your username, email address, display name, and organisation and user identifiers.

4.3 Connected source system metadata

To deliver dx0's core features — search, impact analysis, and AI-powered explanations — we query metadata from the source systems you connect (for example, Salesforce apex classes, flows, field definitions, configuration, and other structural information). This is configuration data about how your systems are built, not business records such as opportunities, contacts, or issue content.

4.4 AI processing

dx0 uses OpenAI's API to generate analysis and explanations. When you use an AI feature, targeted metadata snippets relevant to your question are transmitted to OpenAI. We do not send your full metadata index, OAuth tokens, or any credential material to OpenAI.

4.5 Query results

dx0 includes a SOQL query interface for connected Salesforce accounts. When you run a query, the results pass through dx0's servers and are returned to you. Query results are not sent to any AI model unless you explicitly paste them into the chat interface.

4.6 Usage and technical data

We collect application logs and usage data to maintain Service performance, detect errors, and improve our Service.

5. **HOW WE USE YOUR PERSONAL DATA**

5.1 We use the Personal Data we collect to:

a) provide, operate, and maintain the Service;

b) authenticate users and manage access to connected source systems;

c) generate metadata analysis, security assessments, and AI-powered intelligence;

d) monitor system performance and detect errors;

e) communicate with you about your account, support, and product updates;

f) evaluate and improve the accuracy of AI-generated responses (which may require reviewing AI agent conversations that incidentally contain Personal Data drawn from Customer's connected source systems, where necessary to determine whether a response was correct), and otherwise improve the Service and plan future enhancements using de-identified or aggregated data.

g) meet our obligations under ISO 27001 and applicable law.

6. **LEGAL BASIS FOR PROCESSING (GDPR)**

7.

Purpose	Categories of Data	Legal Basis
Providing and managing user accounts	Account and authentication data	Contract performance — necessary to provide the Service you signed up for
Delivering the core metadata intelligence service	Source systems metadata	Contract performance — core to delivering metadata intelligence
Generating AI-powered assessments and analysis	AI processing of metadata snippets	Contract performance — required to generate assessments and analysis
Operating the data query and reporting feature	Query results (SOQL interface)	Contract performance — required to operate the query feature
Maintaining, securing, and improving the Service	Usage and error logs	Legitimate interests — to maintain, secure, and improve the Service
Information security management and regulatory compliance	Security incident records and ISMS audit logs	Legitimate interests / legal obligation — to operate our ISO 27001-certified ISMS and meet security obligations
Infrastructure security monitoring and audit trail maintenance	CloudTrail, S3 access logs, GuardDuty findings (365-day retention)	Legitimate interests — tamper-evident infrastructure audit trail retained for security and incident response purposes, independently of customer data deletion
Retaining minimal account records following service termination	Preserved account and workspace records post-deactivation	Legitimate interests — retained in minimal form to support account re-activation and anonymous-aggregate product analytics; contain no Salesforce content
Providing AI agent/agent.dx0.io service	Source system metadata, query results and data from user's source system environment.	Legitimate interests – where these categories include Personal Data it is processed (i) to detect and investigate potential abuse, such as attempts to use the product for unauthorised access to or exfiltration of a source system environment; (ii) to monitor for security incidents; (iii) to carry out gap analyses in respect of

Purpose	Categories of Data	Legal Basis
		the functioning of the product; and (iv) to improve the product based on real usage patterns.

8. DATA SHARING

8.1 General

We restrict access to your Personal Data to employees, contractors, and agents who need such access in order to operate, develop, or improve our Service. These individuals are bound by confidentiality obligations and may be subject to discipline, including termination, civil litigation and/or criminal prosecution, if they fail to meet these obligations.

If our Business is acquired or merged with another entity, your Personal Data may be transferred to the new owners/acquirer in connection with that transaction and/or so that we may continue to provide the Service to you. If we become involved in a merger, acquisition, or any form of sale of some of all of our assets, your Personal Data will not be transferred to any third party unless there are adequate safeguards in place with the recipient in respect of the security of your Personal Data.

Your Personal Data may be disclosed to a third party if we are required to do so because of an applicable law, court order or governmental regulation, or if such disclosure is otherwise necessary in support of any criminal or other legal investigation or proceeding in Ireland or abroad.

We share your Personal Data with our third party suppliers who assist us in the provision of the Service. We share Personal Data specifically with the sub-processors listed on our Sub-processors page, under strict confidentiality and data processing agreements which are compliant with Article 28 of the GDPR.

Our approach to data location

HappySoup is an Irish-registered, EU-headquartered company. Where possible, we choose EU/EEA regions for our core infrastructure providers, including our primary database (MongoDB Atlas) and object storage (AWS S3), so that Personal Data is stored within the EEA by default. Certain processing activities, however, necessarily involve providers or infrastructure located outside the EEA — most notably our AI sub-processor, OpenAI. The following sections set out where and why Personal Data may leave the EEA, and the safeguards we apply in each case.

8.2 OpenAI data handling

Because OpenAI operates in the United States, your Personal Data leaves the EEA when AI features are used (via remote access). We rely on OpenAI's Standard Contractual Clauses (SCCs) as the transfer mechanism for these processing purposes. The specific OpenAI data handling commitments relevant to our customers are:

8.3 Limited Use (AI models)

API inputs are not used to train OpenAI's models. This applies to metadata snippets and conversation content. We use the OpenAI API tier, not ChatGPT or any consumer product.

8.4 Abuse-monitoring retention: 30 days

OpenAI retains API request data for abuse detection for up to 30 days, after which it is automatically deleted. Access is restricted to authorised OpenAI personnel investigating suspected misuse.

8.5 Application-state retention: 30 days

We use OpenAI's Responses API with conversation logging enabled. Each conversation turn is accessible in OpenAI's Logs UI for 30 days, then auto-deleted. This cannot be deleted on demand before the 30-day window expires.

OpenAI does not offer EU data residency for API inference to non-enterprise customers. We are not currently enrolled in OpenAI's Zero Data Retention (ZDR) programme.

9. INTERNATIONAL DATA TRANSFERS

Your Personal Data may be transferred to, stored at, or accessed from a destination outside the EEA (a 'third country') for the purposes of us providing the Service. It may also be processed by staff operating outside the EEA who work for us or any of our suppliers. We will take all steps reasonably necessary to ensure that your Personal Data is treated securely and to an acceptable EU standard. The safeguards in place with regard to the transfer of your Personal Data to third countries shall include (but shall not be limited to) reliance by us on a decision of the European Commission confirming an adequate level of data protection in the respective third country, the entry by us into appropriate contracts with third parties incorporating standard contractual clauses approved by the European Commission where required or reliance other appropriate safeguards and the carrying out of risk assessments and adoption of supplementary and/or mitigating measures to ensure compliance with Data Protection Laws.

For the current list of sub-processors, their locations, and transfer mechanisms, see our Sub-processors page.

10. DATA RETENTION

The table below summarises how long each category of Personal Data is retained by us. The full per-category schedule, storage locations, and deletion triggers are documented in the Data Retention section of our Security Page.

Data	Retention
Account information (name, email, company)	Account lifetime; removed on erasure request
Session data	7-day fixed TTL
Salesforce OAuth tokens	Until organisation disconnected, workspace deleted, or account deactivated
Salesforce metadata index	Overwritten on each re-index (every 6 hours or on demand); fully purged on org

Data	Retention
	disconnect, workspace delete, or account deactivation
AI conversations	Lifetime of the workspace; purged on workspace delete or account deactivation; individual conversations deletable by the user at any time
OpenAI copy of conversation data	Up to 30 days on OpenAI's systems, independently of deletion on our system
Workspace configuration and activity logs	Until workspace deleted or account deactivated
Preserved account/workspace records post-deactivation	Retained in minimal form until erasure is requested; contain no Salesforce content
CloudTrail, S3 access logs, GuardDuty findings	365 days; not subject to user deletion triggers

11. **TERMINATION**

When a connected source system is disconnected, we revoke the associated OAuth session (or equivalent authentication credential) and purge all data scoped to that connection. When a workspace is deleted or a trial expires, all user data in that workspace is purged. When an account is deactivated, the same cascade runs across all workspaces. The account, workspace, and user records themselves are preserved in minimal form for re-activation and aggregate analytics; they contain no Salesforce content and are removed in full upon an erasure request.

12. **COOKIES POLICY**

A cookie is a small text file that is placed on your device by a web server, which we store on your browser or the hard drive of your computer if you agree. Cookies contain information that is transferred to your computer's hard drive. Our Website uses cookies to distinguish you from other users of our Website. This helps us to provide you with a better experience when you browse our Website and also allows us to improve the Website/mobile application. Cookies also help us to improve our Service and to deliver many of the functions that make your browser experience more user-friendly.

We use the following types of cookies:

Strictly necessary cookies

These cookies are required for the operation of our Website. They include, for example, cookies that enable you to log into secure areas of our Website, use a shopping cart or make use of e-billing services.

Analytical or performance cookies

These cookies allow us to recognise and count the number of visitors and to see how visitors move around our Website when they are using it. This helps us to improve the way our Website

works, for example, by ensuring that users are finding what they are looking for easily and to see how effective and relevant advertising on our Website is.

Functional cookies

These cookies are used to recognise you when you return to our Website. This enables us to personalise our content for you, greet you by name and remember your preferences (for example, your choice of language or location) and remember if we have already asked you for feedback or to complete a survey.

Targeting cookies

These cookies record your visit to our Website, the pages you have visited and the links you have followed. We will use this information to make our Website and the advertising displayed on them more relevant to your interests. We may also share this information with third parties for this purpose.

Cookies used on this Website

Cookies on our Website are placed both by us (first party) and by third parties whose services we use, such as web traffic analysis, hosting infrastructure, and customer support tools. A full, current list of all cookies used — including the provider, purpose, category, and duration of each — is available in our Cookie Declaration, which updates automatically whenever our cookie usage changes.

The 'Help' menu bar of most browsers will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie and how to disable cookies altogether. You can also disable or delete similar data used by browser add-ons, such as flash cookies, by changing the add-ons settings or visiting the website of its manufacturer.

Further information about browser privacy settings, and cookies and how to disable them can be found at www.allaboutcookies.org or www.ico.org.uk/your-data-matters/online/cookies. You can block cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies), you may not be able to fully experience the interactive features of our Service/Website/mobile application or other related websites/mobile applications which you visit/use.

13. YOUR RIGHTS

As a data subject, you have the following rights under Data Protection Laws and we, as controller in respect of your Personal Data, will comply with such rights in respect of your Personal Data. These rights are explained in more detail below, but if you have any comments, concerns or complaints about our use of your Personal Data, please contact us.

We will respond to any rights that you exercise within one month of receiving your request, unless the request is particularly complex, in which case we will respond within three months (we will inform you within the first month if it will take longer than one month for us to respond).

To exercise any of these rights, contact us at help@happysoup.io. We will respond within 30 days.

Right	Further Information
Right of Access (Article 15 GDPR)	You have the right to request a copy of your Personal Data. Requests for your Personal Data must be made to us specifying what Personal Data you need access to, and a copy of such request may be kept by us for our legitimate purposes in managing the Service. To help us find the information easily, please give us as much information as possible about the type of information you would like to see. If, to comply with your request, we would have to disclose information relating to or identifying another person, we may need to obtain the consent of that person, if possible. If we cannot obtain consent, we may need to withhold that information or edit the data to remove the identity of that person, if possible. We are also entitled to refuse a data access request from you where (i) such request is manifestly unfounded or excessive, in particular because of its repetitive character (in this case, if we decide to provide you with the Personal Data requested, we may charge you a reasonable fee to account for administrative costs of doing so); or (ii) we are entitled to do so pursuant to Data Protection Laws. For security reasons, we will take reasonable steps to confirm your identity before providing you with any Personal Data we may hold about you.
Right of Rectification (Article 16 GDPR)	You have the right to request that we amend any inaccurate or incomplete Personal Data that we have about you. If you would like to do this, please (i) email or write to us; (ii) let us have enough information to identify you (e.g. name, registration details); and (iii) let us know the information that is incorrect and what it should be replaced with. If we are required to update your Personal Data, we will inform recipients to whom that Personal Data have been disclosed (if any), unless this proves impossible or has a disproportionate effort. It is your responsibility that all of the Personal Data provided to us is accurate and complete. If any information you have given to us changes, please let us know as soon as possible.
Right to Object (Article 21 GDPR)	You have the right to ask us to stop using your Personal Data, and we will comply unless there is a legal basis for us to continue using it, which we will explain to you.
Right to Erasure (Article 17 GDPR)	You can ask us to erase your Personal Data (i) where we do not need your Personal Data in order to process it for the purposes set out in this Policy; (ii) if you had given us consent to process your Personal Data, you withdraw that consent and we cannot otherwise legally process your Personal Data; (iii) you object to our processing and we do not have any legal basis for continuing to process your Personal Data; (iv) your Personal Data has been processed unlawfully or have not been erased when it should have been; or (v) the Personal Data have to be erased to comply with law.

	We may continue to process your Personal Data in certain circumstances in accordance with Data Protection Laws. Where you have requested the erasure of your Personal Data, we will inform recipients to whom that Personal Data has been disclosed, unless this proves impossible or involves disproportionate effort. We will also inform you about those recipients if you request it.
Right to Restriction of Processing (Article 18 GDPR)	You may request that we stop processing your Personal Data temporarily if (i) you do not think that your Personal Data is accurate (but we may start processing again once we have checked and confirmed that it is accurate); (ii) the processing is unlawful but you do not want us to erase your Personal Data; (iii) we no longer need the Personal Data for our processing; or (iv) you have objected to processing because you believe that your interests should override the basis upon which we process your Personal Data. If you exercise your right to restrict us from processing your Personal Data, we will continue to process the Personal Data if: (i) you consent to such processing; (ii) the processing is necessary for the exercise or defence of legal claims; (iii) the processing is necessary for the protection of the rights of other individuals or legal persons; or (iv) the processing is necessary for public interest reasons.
Right to Data Portability (Article 20 GDPR)	You may ask for an electronic copy of your Personal Data that you have provided to us and which we hold electronically, or for us to provide this directly to another party. This right only applies to Personal Data that you have provided to us – it does not extend to data generated by us. In addition, the right to data portability also only applies where (i) the processing is based on your consent or for the performance of a contract; and (ii) the processing is carried out by automated means.
Right to be Informed	You have the right to clear, transparent and easily understandable information about your rights and about how we use your Personal Data. We use this Policy to inform you of your rights.
Right to Withdraw Consent	Where processing is based on your consent, you have the right to withdraw your consent at any time with future effect by contacting us. However, if you do withdraw your consent we may not be able to continue to provide the Service.
Rights in relation to automated decision making	We do not attempt to collect further data without user consent that enables personally identifiable profiling of our users.
Right to Complain to the DPC	If you do not think that we have processed your Personal Data in accordance with this Policy, please contact us in the first instance (see 'How to Contact Us' below). If you are not satisfied, you can complain to the DPC or exercise any of your other rights pursuant to Data Protection Laws. Information about how to do this is available on the DPC website at https://www.dataprotection.ie.

14. **SECURITY**

We implement technical and organisational measures appropriate to the risk, including AES-256 and AWS KMS encryption at rest, TLS 1.2+ in transit, AWS KMS envelope encryption for Salesforce OAuth tokens, server-side session management, and independent penetration testing. dx0 is ISO 27001 certified (Certificate No. 26ISMS-1158, Glocert International, 2026). For full detail, see our Security Page.

15. PRODUCT AND MARKETING COMMUNICATIONS

Where you engage with dx0 in a business context, including by requesting, evaluating or participating in a trial of our services, we may use the business contact information you provide to send you communications about dx0, such as product updates, educational content, new features and other information relevant to your use or evaluation of our services.

dx0 trials are not offered on a self-service basis. They generally follow direct engagement with our team and may involve product demonstrations, commercial discussions, confidentiality agreements or legal and security review. In this context, we may process your business contact information on the basis of our legitimate interests in maintaining and developing our business relationship with you, where permitted by applicable law.

We aim to keep these communications relevant to your professional relationship with dx0. You can opt out of marketing communications at any time using the unsubscribe link included in our emails or by contacting us. We will respect any such objection or opt-out.

16. CHILDREN'S PRIVACY

dx0 is a professional B2B tool and is not intended for use by anyone under the age of 18. We do not knowingly collect Personal Data from minors. If we become aware that we have received Personal Data from or about a person under the age of 18, we will delete such information from our records.

17. CHANGES TO THIS POLICY

We may update this Policy from time to time. If changes are material, we will notify you by email or through the application. The "Last updated" date at the top of this page reflects the most recent revision.

18. HOW TO CONTACT US

For questions about this Policy or how we handle your data:

HappySoup Limited
Dublin 15, Ireland

help@happysoup.io

19. CHANGE LOG

20.

Date	Description of Change
7th July, 2026	Initial version of revised policy.
15th July, 2026	Clarified Section 5.1(f) to specify that improving the Service using Personal Data is limited to evaluating and correcting the accuracy of AI-generated responses; all other service improvement activity uses de-identified or aggregated data only.
11th August, 2026	Added Section 15 regarding policies for product and marketing communications using business contact information.