

Data Processing Agreement

Last updated: 2 Aug 2026

FullEnrich · fullenrich.com · The authoritative version of this document lives at fullenrich.com and may be updated there.

Preamble

This Personal Data Processing Agreement (hereinafter "DPA") is entered into between FullEnrich and the Client, as defined in the General Terms and Conditions of Use and Sale. This DPA incorporates by reference the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, which automatically apply to international transfers of personal data.

Terms beginning with a capital letter have the same definition as given in the General Terms and Conditions of Use and Sale.

The DPA applies to the processing of personal data carried out by FullEnrich for the Client, in the context of the Client's use of the Software accessible from FullEnrich's website (<https://fullenrich.com> and <https://app.fullenrich.com>) and the FullEnrich API.

1 - Purpose

The purpose of this DPA is to ensure compliance of personal data processing carried out by FullEnrich for the Client with paragraphs 3 and 4 of Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "GDPR").

It is understood that FullEnrich acts on behalf of the Client and on documented instructions from the latter. The Client acts either on its own behalf and for its own purposes as a data controller or on behalf and for the purposes of its own clients as a data processor.

2 - Description of Processing Activities

The processing activities carried out by FullEnrich for the Client have the following characteristics:

Categories of data subjects: the Client's prospects, candidates, or the Client's customers' prospects and candidates. These are business professionals;

Categories of personal data processed: identity and contact data of prospects and candidates. This may potentially include data related to their professional activities, such as their roles or companies;

Nature of processing: enrichment processing of data provided by the Client, temporary data storage;

Purposes for which personal data are processed: enrichment performed so that the Client or the Client's Customers can conduct commercial prospecting operations or recruitment activities;

Duration of processing: default storage for 3 months followed by automatic deletion.

FullEnrich processes personal data only for the purposes of the processing.

3 - Instructions

FullEnrich processes personal data only on documented instructions from the Client, unless required to do so by Union or French law. In such cases, FullEnrich shall inform the Client of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest.

FullEnrich shall inform the Client if, in its opinion, an instruction given by the Client infringes the GDPR or applicable data protection regulations.

To support Client's compliance with the California Consumer Privacy Act (CCPA) and similar US state privacy laws, FullEnrich will not:

- Sell personal data provided by the Client;
- Process personal data provided by the Client for any purpose other than for the specific purposes set forth herein. For the avoidance of doubt, FullEnrich will not process personal data outside of the direct business relationship between Client and FullEnrich;
- Attempt to link, identify, or otherwise create a relationship between personal data provided by the Client and non-personal data or any other data without the express authorization of the Client.

4 - Processing Security

FullEnrich implements the technical and organizational measures specified in Appendix 1 to ensure the security of personal data. These measures include, in particular, protection against any security breach leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of personal data, or unauthorized access to such data.

When assessing the appropriate level of security, FullEnrich takes into account the state of the art, implementation costs, and the nature, scope, context, and purposes of processing, as well as the risks to data subjects.

FullEnrich grants its personnel access to personal data being processed only to the extent strictly necessary for the execution, management, and monitoring of processing. FullEnrich ensures that they commit to maintaining confidentiality.

5 - Documentation and Compliance

FullEnrich makes available to the Client all information necessary to demonstrate compliance with the obligations set forth in this DPA.

At the Client's request and in the presence of indications of non-compliance, FullEnrich also allows for audits of processing activities covered by this DPA. This audit may be carried out by the Client itself or by an independent auditor it mandates. The audit is conducted with 30 days' notice sent by the Client to FullEnrich.

FullEnrich makes available to the competent supervisory authority, upon request, the information set out in this article, including the results of any audit.

6 - Use of Sub-processors

FullEnrich has the Client's general authorization regarding the recruitment of sub-processors based on an agreed list, present in the Appendix. FullEnrich specifically informs the Client by any means of any planned changes to this list through the addition or replacement of sub-processors at least eight (8) days in advance, thus allowing the Client to object to these changes before the recruitment of the concerned sub-processor(s).

When FullEnrich engages a sub-processor to carry out specific processing activities, it ensures that the sub-processor has similar data obligations to those imposed on FullEnrich by this DPA.

FullEnrich remains fully responsible to the Client for the performance of the sub-processor's obligations under the contract concluded with the latter.

7 - International Transfers

Any transfer of personal data to a third country or international organization by FullEnrich is only carried out based on documented instructions from the Client or to meet a specific requirement of Union or French law and is conducted in accordance with Chapter V of the GDPR.

When the Client's use of FullEnrich services involves transfers of personal data outside the European Economic Area, such transfers shall be governed by the Standard Contractual Clauses adopted by the European Commission (Commission Implementing Decision (EU) 2021/914), which are hereby incorporated by reference and form an integral part of this DPA ("SCC").

By accepting this DPA, the Client automatically becomes a party to the SCC as a data exporter, with FullEnrich acting as data importer. The Client's specific details (name, address, contact information) are those provided in their FullEnrich account and are incorporated into the SCC by reference. The SCC shall apply automatically to any such international transfers without requiring separate execution.

The Client agrees that when FullEnrich engages a sub-processor in accordance with Article 6 and the processing activities involve a transfer of personal data within the meaning of Chapter V of the GDPR, FullEnrich and the sub-processor may frame this transfer using the same standard contractual clauses.

8 - Assistance to the Client

FullEnrich shall promptly inform the Client when it receives a request to exercise rights from a data subject. FullEnrich assists the Client in responding to requests from data subjects to exercise their rights, taking into account the nature of the processing. FullEnrich complies with the Client's instructions.

However, when it comes to an opt-out request made through FullEnrich's website via the "Do not sell my information" module, the request is deemed to be directly addressed to FullEnrich. In this case, FullEnrich grants the data subject's request without having to notify the Client.

FullEnrich assists the Client in ensuring compliance with the following obligations, taking into account the nature of the processing and the information available to FullEnrich:

The obligation to carry out an assessment of the impact of intended processing operations on personal data protection when a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

The obligation to consult the competent supervisory authority prior to processing when a data protection impact assessment indicates that the processing would present a high risk if the Client or its client did not take measures to mitigate the risk;

The obligations provided for in Article 32 of the GDPR.

9 - Notification of Personal Data Breaches

In case of a personal data breach related to data processed by FullEnrich, it shall inform the Client without undue delay after becoming aware of it.

This notification shall contain:

A description of the nature of the breach (including, where possible, the categories and approximate number of data subjects concerned and personal data records affected);

The contact details of a point of contact where more information can be obtained about the personal data breach;

The likely consequences and measures taken or proposed to be taken to address the breach, including measures to mitigate its possible adverse effects.

When it is not possible to provide all information at the same time, the initial notification shall contain the information available at that time, and further information shall be provided subsequently as it becomes available without undue delay.

10 - Data Fate

Following the termination of the General Terms and Conditions of Use or Sale or the DPA, the Contract ends. Following the end of the Contract, FullEnrich deletes all personal data processed on behalf of the Client, unless Union or French law requires longer retention.

11 - Termination

In the event of FullEnrich's breach of obligations under this DPA, the Client may instruct FullEnrich to suspend the processing of personal data until the latter complies with these clauses or until the Contract is terminated in accordance with Article 15 of the General Terms and Conditions of Use or Sale. FullEnrich shall promptly inform the Client if it is unable to comply with these clauses for any reason.

The Client may terminate this DPA if processing has been suspended and compliance is not restored within two months of suspension.

FullEnrich may terminate the DPA when, after informing the Client that its instructions violate the GDPR and data protection regulations, the Client insists that its instructions be followed.

Appendix 1: Technical and Organizational Security Measures

To ensure data security in accordance with Article 32 of the GDPR, FullEnrich implements technical and organizational measures. These measures are designed to protect personal data against any unauthorized or unlawful processing, accidental loss, destruction, or damage.

Security measures are taken considering the nature, scope, context, and purposes of our processing activities, as well as the risk to the rights and freedoms of data subjects.

Personal Data Pseudonymization and Encryption Measures

FullEnrich uses robust encryption methods, such as bcrypt with a cost of 14 rounds, for password encryption to ensure the security of user credentials. Additionally, FullEnrich uses pseudonymization techniques, such as anonymized logging with user identifiers, to enhance data protection and minimize risks to data subjects' privacy.

Measures to Ensure Ongoing Confidentiality, Integrity, Availability, and Resilience of Processing Systems and Services

FullEnrich ensures processing system resilience through secured databases connected to a virtual private cloud (VPC). This approach protects against unauthorized access and ensures data availability and integrity.

Regular Testing, Assessment, and Evaluation Processes for Technical and Organizational Measures

The security framework includes regular unit and integration testing, as well as continuous evaluation of our technical measures. This proactive approach ensures the ongoing effectiveness of security practices in protecting data during processing.

User Identification and Authorization Measures

We implement secure user identification and authorization mechanisms, including session cookies (JWT) signed with HMAC using the SHA256 algorithm. Role-based access control (RBAC) is strictly enforced for each user action, ensuring access rights are properly managed and restricted.

Data Protection Measures During Transmission

All data transmissions are secured via HTTPS/SSL tunnels, extending robust encryption from the user endpoint to our databases. This ensures data confidentiality and integrity in transit.

Data Protection Measures During Storage

Data at rest is protected by AES encryption, a widely recognized standard that provides a high level of security for stored data.

Measures to Ensure Physical Security of Locations Where Personal Data are Processed

Our data hosting provider, DigitalOcean, is compliant with SOC 2 and ISO 27001 standards, ensuring physical security measures are in place to protect against unauthorized data access.

Event Logging Measures

We maintain comprehensive access logs, including IP addresses, user IDs, actions taken, and roles. These logs are encrypted at rest and retained for one year, supporting both security monitoring and compliance requirements.

Data Minimization Measures

Adherence to data minimization principles is ensured through a rigorous data registry, which justifies the collection and processing of each data element, in alignment with the "data minimization" principle.

Limited Data Retention Measures

Data retention policies are strictly enforced, with each dataset being assigned a creation and expiration date. This approach is balanced against legitimate interests to ensure compliance with applicable legal and regulatory requirements.

Technical and Organizational Measures for (Sub-)Processors

For transfers to (sub-)processors, we require the implementation of specific technical and organizational measures enabling the (sub-)processor to effectively assist the data controller. These measures include, among others, encryption of personal data, ensuring confidentiality, integrity, availability, and resilience of processing systems and services, as well as compliance with data minimization and retention policies.

Related documents

- [List of sub-processors](#)
- [Standard Contractual Clauses](#)

