

NeuroDisplay Data Processing Agreement — Professional Customers

Version: dpa-b2b-2026-08-en-v1

Effective date: 2026-08-01

sha256:c7fea23c3aade8639363272a3ae9e93292ffa08cf6e83ad15ce468399b2f0e24

This Data Processing Agreement (“DPA”) is part of the contract concluded between A2Display and the Professional Client. It applies when A2Display processes personal data on behalf of the Client within the framework of NeuroDisplay.

1. Purpose and scope

The DPA defines the obligations of the Parties in accordance with Article 28 of the GDPR. It covers the treatments described in Appendix II and takes precedence, for these treatments, over any contradictory stipulation of lower rank.

2. Roles of the Parties and documented instructions

The Client acts as data controller for the content, paths, configurations and data that he decides to process in NeuroDisplay. A2Display acts as a subcontractor for these operations and only processes this data on documented instructions from the Client, including for transfers, unless applicable legal obligation.

A2Display acts separately as data controller for account management, security, commercial relations, billing, Support and its legal obligations. These treatments are described in the Privacy Policy.

3. Lawful instructions and responsibility of the Customer

The Client guarantees the lawfulness of its instructions, the relevance of the data, the information of the people and the existence of a legal basis. It does not use the Service to unnecessarily process sensitive data. A2Display informs the Client when an instruction appears to violate applicable law, unless prohibited by law.

4. Duration

The DPA applies for the duration of the contract and until the deletion or restitution of the data processed for the Customer, subject to legal retention obligations and technical backup cycles.

5. Confidentiality and authorized personnel

A2Display limits access to those who need it to provide, secure or support the Service. These people are subject to an appropriate obligation of confidentiality and access management rules.

6. Security of processing

A2Display implements the appropriate measures described in Appendix III, taking into account the state of the art, costs, nature, scope, context and risks. No certification not obtained by A2Display is claimed.

7. Sub-processors

The Customer generally authorizes sub-processors listed in the active version of the public list. A2Display imposes appropriate protection obligations and remains responsible for their subcontracting obligations under the conditions of applicable law.

A2Display will notify Customers of a material change by a reasonable means. The Customer may raise an objection motivated by data protection; the Parties then seek a reasonable solution.

8. International transfers

Some providers may process data or allow access from countries outside the European Economic Area. Depending on the case, transfers are based on an adequacy decision, standard contractual clauses or another applicable guarantee. No exclusively European residency is promised without proof linked to the active configuration.

9. Rights of individuals

Taking into account the nature of the processing, A2Display provides the Client with reasonable assistance in responding to requests for access, rectification, erasure, limitation, opposition and portability. A2Display transmits to the Client any request clearly relating to data processed on its behalf, unless otherwise instructed or required.

10. Compliance assistance

A2Display reasonably assists the Client with security, impact analyzes and prior consultations, taking into account the information available and the nature of the Service. An unusual or important service may be subject to reasonable conditions agreed in advance.

11. Personal data violations

When A2Display confirms a violation affecting data processed for the Client, A2Display informs the Client without undue delay and progressively provides useful available information. The Customer remains responsible for his notifications as data controller.

12. Restitution, export and deletion

During the contract, the Customer uses the available export functions. After the end of the contract, a thirty day access or export window may be provided. Data from active systems is deleted within thirty days following this window, unless required by law or justified freezing.

Backup copies expire according to the vendor's technical cycles, are not reused for business purposes, and deletions are reapplied after restoration when required. It is not promised that an encrypted backup will be rewritten immediately for an isolated line.

13. Information, audits and evidence

A2Display makes available information reasonably necessary to demonstrate compliance with this DPA. Audits are planned, proportionate, subject to confidentiality and designed to avoid compromising other Customers or the security of the Service. Available independent reports or documentary evidence are preferred.

14. Liability and contractual order

Liability linked to the DPA is governed by the lawful limitations provided for in the contract, without reducing the imperative rights of individuals or the obligations which cannot be limited. In the event of a contradiction, the DPA prevails for the protection of the data processed for the Customer.

15. Evolution and contact

The DPA is versioned. A material modification is notified and may require new acceptance by an Owner or authorized representative, without retroactive effect. Requests use the NeuroDisplay form, "Data Protection" category, or NeuroDisplay Support for Authenticated Customers. A2Display does not claim to have appointed a DPO.

16. Annex I — Parts

Subcontractor: A2Display, simplified joint stock company, operator of NeuroDisplay, 1 rue de la Caillardi re, 49070 Beaucouz , France.

Responsible for processing: the Professional Customer identified in the Organization, the Checkout, the quote or the contract. The representative who accepts the DPA certifies having the authority to bind the Client.

17. Annex II — Description of processing

- Subject: hosting, organization, distribution, support and security of the Client's content and configurations.
- Duration: duration of the contract and deletion period described in article 12.
- Nature: collection, recording, organization, consultation, adaptation, transmission to Players and chosen recipients, backup and deletion.
- Purposes: dynamic display, tactile paths, administration, support, security and functions requested by the Customer.
- Data: professional identity, accounts and roles, content, media, configurations, technical logs, support data and context-enabled data.
- Persons: Client users, staff, visitors or other persons whose data the Client chooses to process.

18. Annex III — Technical and organizational measures

Established measures include: RLS, RBAC, multi-tenant isolation, server controls, secrets kept on the server side, encryption in transit, vendor storage encrypted according to their capabilities, signed URLs, redacted logs, request_id, Test/Production separation, synthetic test data, cross-org protections, rate limiting, authorization of Player commands, access management, vendor backups and incident procedure.

19. Annex IV — Active subcontractors

The active and versioned list is published on the NeuroDisplay Subcontractors page. It includes Supabase, Vercel, Resend and OpenAI when AI functions are active. Open-Meteo is temporarily disabled until a commercial subscription is configured and does not receive any production data.

Cloudflare R2 for Future Document Library, GitHub, Mailosaur, developer tools, and unused providers are not in the active list.

20. Annex V — International transfers

Regions and mechanisms depend on the provider, Plan, and active configuration. Potential transfers outside the EEA use an adequacy decision, standard contractual clauses or other applicable safeguard. The versioned list indicates possible regions and general mechanisms without revealing sensitive configuration.

21. Annex VI — Retention and deletion

- contents, rules, compositions and configurations: contract, thirty-day export, active deletion within the following thirty days;
- temporary files and abandoned uploads: twenty-four hours;
- application logs: ninety days;
- security and authentication logs: one hundred and eighty days;
- technical condition and heartbeat Player: ninety days;
- analytics identifiable by Organization: thirteen months maximum;
- Support tickets and attachments: processing then twelve months after closing;
- AI prompts: not stored in Analytics or permanently, unless explicitly recorded; redacted technical logs: thirty days maximum;
- contractual and accounting proofs: applicable legal durations.

Higher retention is only applied in the presence of a legal obligation, litigation or documented freeze.

22. Annex VII — Assistance and incidents

A2Display maintains a procedure covering detection, classification, containment, preservation of evidence, assessment of people and data, risk analysis, notification of the Client without undue delay, updates, closure and feedback. Exchanges use a request_id and a redacted registry.