

DPIA Statement

Although published in the Remotion documentation, this assessment concerns the [Remotion Pro licensing platform](#) and its licensing telemetry. It explains why that processing is not likely to result in a high risk to individuals, and why a formal Data Protection Impact Assessment is not required. It is provided for transparency and is not a contract or legal advice.

Version 1.0. Effective July 6, 2026

This DPIA Statement explains how **Remotion AG**, Neunbrunnenstrasse 38, 8050 Zürich, Switzerland ("**Remotion**", "**we**", "**us**") has assessed whether the personal data processing carried out by the Remotion Pro licensing platform and its usage telemetry is likely to result in a "high risk" to individuals, and therefore whether a formal Data Protection Impact Assessment ("**DPIA**") is required.

The conclusion of this assessment is that, in its current form, the Remotion Pro licensing platform and its telemetry do **not** trigger a mandatory DPIA under GDPR Article 35 or Swiss nFADP Article 22. This statement documents that conclusion and the reasoning behind it, in line with the accountability principle.

This statement is provided for transparency. It is not a contract and does not create rights or obligations beyond those set out in the [Terms and Conditions](#) ("**Main Agreement**") and the [Privacy Policy](#). It complements the [DPA Statement](#), which explains Remotion's role as an Independent Controller. Where there is any conflict, the Main Agreement and Privacy Policy prevail. This statement is not legal advice.

1. Summary of findings

A DPIA is only mandatory where a processing operation is "likely to result in a high risk to the rights and freedoms of natural persons" (GDPR Article 35(1); Swiss nFADP Article 22(1)). After assessing the licensing platform and telemetry against the criteria used by European and Swiss regulators, Remotion has concluded that this threshold is **not** met. A formal DPIA is therefore not legally required for the platform in its current form.

The key reasons are:

- The personal data Remotion processes (account, billing, store, support, license verification, and telemetry data) is limited operational and commercial metadata, not sensitive data.
- Telemetry counts rendering activity for licensing and billing. It does not profile, score, or monitor the behaviour of individuals over time.
- Remotion has no access to the media, source code, or end-user content that customers render. That content stays in the customer's own environment.
- The processing does not target children or other vulnerable groups, and does not combine datasets to build profiles.

Remotion keeps this assessment under review and will carry out a DPIA if it later introduces processing that is likely to result in a high risk.

2. Scope of this assessment

This assessment distinguishes between the Remotion software and the Remotion Pro licensing platform, because the data protection responsibilities are different for each.

- **The Remotion software (client-side / self-hosted execution):** Remotion is distributed as source-available and commercial packages that run entirely within the customer's own infrastructure or in the end user's browser. When a customer renders a video that contains personal data, the customer determines why and how that data is processed and acts as the Controller. Remotion has no access to, or visibility of, that content. If a customer's own use case involves high-risk processing (for example, biometrics, large-scale profiling, or employee monitoring), it is the customer's responsibility to assess whether a DPIA is required for that use case.

- **The Remotion Pro licensing platform and telemetry:** Remotion acts as an Independent Controller for its website, user accounts, billing profiles, license verification, and the lightweight telemetry it receives to verify commercial licensing tiers and support usage-based billing. This is the processing assessed below.

3. What the platform processes

For the licensing platform, Remotion processes standard business and account identifiers (such as names, business email addresses, billing details, and license keys) as described in the [Privacy Policy](#).

Telemetry is limited to the operational and license metadata described in the [Telemetry section of the Terms](#):

- IP address;
- domain name;
- whether the render was in production or development; and
- whether the render was a video or a still image.

The telemetry system is decoupled from the rendering logic by design. It does **not** collect video names, file paths, media content, input properties, rendered output, or any other user content. Telemetry is also non-blocking: rendering continues to work even if a telemetry request fails.

4. High-risk assessment against regulatory criteria

European and Swiss regulators (the European Data Protection Board, building on the Article 29 Working Party guidelines) identify nine criteria that indicate potentially high-risk processing. As a rule of thumb, processing that meets **two or more** of these criteria is likely to require a DPIA. Remotion's licensing platform and telemetry meet **none** of them.

Criterion	What it covers	Remotion's processing	Met?
Evaluation or scoring	Profiling, performance tracking, or scoring of individuals.	Telemetry only tallies render counts to determine the applicable pricing tier. No profiling or scoring of individuals.	No
Automated decisions with legal or significant effects	Automated decisions that deny a person a contract, employment, or a service.	Telemetry is non-blocking; a failed or missing license check never stops a render.	No
Systematic monitoring	Tracking behaviour, location, or activity over time, including across sites.	Data is captured only at the moment of a single render event, not across sites or over time.	No
Sensitive or special category data	Health, biometric, genetic, political, or criminal-record data.	Only standard business identifiers and basic network metadata are processed.	No
Large-scale processing	High volumes of data subjects, records, or extensive retention.	Each telemetry event is a small set of metadata attributes, not a behavioural data lake.	No
Matching or combining datasets	Merging datasets to profile people in unexpected ways.	Telemetry is not cross-referenced or combined with external marketing or profiling datasets.	No
Vulnerable data subjects	Children, employees, patients, or others in a power imbalance.	The platform is a business-to-business developer tool; it does not target children or vulnerable groups.	No
Innovative use of new technology	Novel technologies such as facial recognition or AI behavioural analysis.	License verification uses standard, well-established request logging.	No
Preventing the exercise of a right or use of a service	Processing that blocks access to a contract, service, or right.	Standard commercial licensing; it does not restrict access to alternatives or to legal rights.	No

Because none of the nine criteria are met, the processing does not cross the high-risk threshold that would make a DPIA mandatory under GDPR Article 35.

5. Swiss nFADP considerations

As a company based in Zürich, Remotion is also subject to the revised Swiss Federal Act on Data Protection (nFADP) and the supervision of the Federal Data Protection and Information Commissioner (FDPIC). The nFADP mirrors the GDPR's risk-based approach: a DPIA (a "data protection impact assessment" under Article 22 nFADP) is required only where processing is likely to result in a high risk to the personality or fundamental rights of the people concerned.

The same analysis applies. Because the telemetry collects only standard system and licensing metadata, and does not track individuals' behaviour, location, or private sphere, it does not present a high risk to personality rights under the nFADP, and no DPIA is required on that basis either.

To support its obligations under both regimes, Remotion maintains a record of its processing activities, provides clear information about what data is collected and why, and puts appropriate cross-border data transfer mechanisms in place with its service providers (see the [DPA Statement](#)).

6. Data flows and the dual role of payment processors

To operate the licensing platform, Remotion relies on a set of service providers. A current, itemized list of those providers, including their location and high-level purpose, is published in the [Service providers section of the DPA Statement](#). At a high level, the personal data Remotion handles for the licensing platform flows to the categories of provider below.

Provider category	Jurisdiction	Role
Cloud hosting and content delivery	US / EU / global	Processor (on Remotion's instructions)
Error monitoring and diagnostics	EU	Processor (on Remotion's instructions)
Payment and subscription processing	IE (EU) / US	Processor and, for its own compliance purposes, Independent Controller
Transactional email, newsletter, and support	US / EU	Processor (on Remotion's instructions)
Compliance assessment	CH / EU	Processor (on Remotion's instructions)

These transfers keep the platform's processing low-risk: the data shared with each provider is limited to what that provider needs, and providers acting on Remotion's behalf are bound by data processing agreements and appropriate transfer safeguards.

The dual role of payment processors

Payment providers (such as Stripe) act in two distinct roles, which is common in the payments industry:

- **As a Processor**, when handling subscriptions, recurring payments, and invoicing on Remotion's instructions.
- **As an Independent Controller**, when performing identity verification, fraud monitoring, and anti-money-laundering or sanctions screening for their own legal obligations.

This split matters for the risk assessment: the higher-risk activities associated with financial profiling and fraud prevention are carried out by the payment processor as an Independent Controller under its own terms, not by Remotion. Remotion does not receive or process that profiling data.

7. Mitigations and privacy-by-design measures

Even though a DPIA is not required, Remotion applies privacy-by-design measures to keep the residual risk low:

- **Data minimization:** Telemetry is restricted to the limited operational metadata listed above and is decoupled from rendered content.
- **Retention and anonymization:** Remotion is implementing a retention and anonymization schedule for telemetry data, including IP addresses, so that identifiable data is not kept longer than necessary for billing and abuse prevention.

- **Transparency:** What is collected and why is documented in the Privacy Policy, the Terms, the [DPA Statement](#), and this statement.
- **Customer responsibilities:** Where a customer's integration causes personal data of the customer's own end users (for example, end-user IP addresses or technical identifiers) to be transmitted to Remotion through client-side rendering, the customer is responsible for providing any notices and obtaining any consents required under applicable data protection law, including referencing Remotion's telemetry in the customer's own privacy notices where required. This is also explained in the [Privacy Policy](#) and the [DPA Statement](#).
- **Contracts with service providers:** Providers acting on Remotion's behalf are bound by data processing agreements and appropriate international transfer safeguards.
- **Enterprise arrangements:** Enterprise customers with specific data protection requirements can request a tailored arrangement; see the [DPA Statement](#).

8. Decision and review

Based on the assessment above, Remotion concludes that the Remotion Pro licensing platform and its telemetry, in their current form, are **not** likely to result in a high risk to individuals, and that a formal DPIA is **not** required under GDPR Article 35 or Swiss nFADP Article 22.

Remotion will revisit this decision and carry out a DPIA if it materially changes how it processes personal data, for example by introducing a hosted rendering service, profiling, or other high-risk processing.

9. Contact

Privacy contact: privacy@remotion.dev **Security contact:** security@remotion.dev

Remotion AG, Neunbrunnenstrasse 38, 8050 Zürich, Switzerland. Contact: privacy@remotion.dev