WORKING PAPER · Copyright, data protection and AI regulation (Türkiye / EU)
Prepared 31 October 2026 · Revised 2 November 2026 · Version 2.0
DOI: https://doi.org/10.5281/zenodo.23896353

Software Rights, Cross-Border Data Transfers and EU AI Act Obligations for AI and SaaS Ventures in Türkiye

Av. Dr. Alihan Sağır
Ph.D. in Private Law · Sağır Hukuk Bürosu, Antalya, Türkiye
ORCID: 0000-0002-3267-3838 · Author profile

Abstract

An AI or SaaS venture may develop its own code, incorporate third-party software and models, and send customer data to external infrastructure. Each choice raises a distinct question about its ability to offer the resulting service. I examine how Turkish copyright rules establish the scope of protection and the venture's authority to use software, how Article 9 KVKK governs cross-border personal-data flows, and how upstream licences condition distribution and network use. I then consider when the EU AI Act applies to a venture established in Türkiye and how its role determines the relevant duties and application dates. The analysis links those questions through the development and deployment of a single service: software rights, permission to process and transfer personal data, and regulatory responsibility each require their own legal basis.

Keywords: Artificial intelligence law; SaaS; Software copyright; Software licensing; KVKK Article 9; AGPLv3; EU AI Act

Scope and method

I examine the legislation applicable as of the date of this study through a doctrinal analysis of the Turkish Law on Intellectual and Artistic Works No. 5846 (FSEK), the Law on the Protection of Personal Data No. 6698 (KVKK), the relevant software licences, and the EU AI Act as amended by Regulation (EU) 2026/1744. The discussion follows the relationship between developing software, securing the rights needed to offer it, using external infrastructure and components, and supplying an AI-enabled service to the EU market.

1. Expression, software and database protection

The legal basis for commercialising an AI-enabled product begins with identifying which elements can attract protection. A service may combine human-written code, curated datasets, prompts and machine-generated outputs. Those elements require separate treatment under FSEK. Computer programs and preparatory designs leading to a program qualify as literary and scientific works where they bear the individuality of their author (Art. 1/B(a), (g); Art. 2, item 1). The final paragraph of Article 2 excludes the ideas and principles underlying program elements, including interfaces. A concrete prompt text may nevertheless contain original linguistic expression whose protection requires assessment independently of its underlying method. For AI-generated outputs, the human contribution and the expression attributable to it remain central to the assessment.

Datasets raise a further distinction. Original selection or arrangement may attract compilation protection without extending copyright to the underlying raw data (FSEK Art. 6, item 11). Substantial qualitative or quantitative investment in creating, verifying or presenting the contents may also attract the database maker's sui generis right under Additional Article 8. These forms of protection can coexist when their respective conditions are met. The maker's fifteen-year term runs from disclosure to the public, while a substantial new investment requires a separate assessment for a new protection term.

The resulting distinction matters to the venture's rights position. Protection of its code or database does not establish exclusive rights over every idea, input or output used in the service. Nor does identifying a protected work establish that the venture itself is entitled to exploit it. The next question is how the company acquires that authority from the people who create the product.

2. Securing the venture's rights in developed software

An AI or SaaS company usually relies on software produced by employees, founders or independent developers. The classification of their contribution as a protected work therefore leads to a separate issue: the legal basis on which the company can reproduce, modify, distribute or license that work. The creator's relationship with the company matters because statutory authority to exercise economic rights and contractual acquisition operate through different rules.

Under FSEK Art. 18(2), unless a special agreement or the nature of the work indicates otherwise, economic rights over works created by employees in performing their duties are exercised by the employer. The same rule applies to persons constituting the organs of a legal entity acting within their duties. In the latter case, the legal entity exercises the rights. The connection to the relevant duties limits the rule: employment or organ status does not bring every personal creation within it. Authorship and the company's statutory authority to exercise economic rights consequently remain distinct.

Code written before incorporation and contributions by independent developers require their own contractual basis. An assignment of economic rights and a licence to use them have different effects (FSEK Art. 48). For future works, the undertaking contemplated by Article 50(1) must also be distinguished from the dispositive assignment of a completed work under Articles 48 and 52. Written form and individual specification of the rights must be considered at both stages. Signing a development agreement before a module exists does not by itself establish a completed transfer of all rights in that module.

The company's rights position therefore cannot be inferred solely from payment for development or possession of the source code. It depends on who created each contribution, whether it falls within a statutory rule, and which assignments or licences cover the intended uses. That chain of authority establishes the rights the company can exercise over its own product; third-party components remain subject to their separate licences.

3. Personal-data flows and cross-border transfer mechanisms

Once the product is deployed, its operation may depend on foreign cloud infrastructure or model APIs. The authority to use the software does not determine whether customer information can lawfully be sent to those providers. Article 9 KVKK becomes relevant insofar as the flow contains personal data. Genuinely anonymous information must be distinguished from pseudonymised or apparently de-

identified material that remains linkable to an individual. The controller and processor roles must also be identified for each flow, including any processing by the provider for its own purposes (KVKK Arts. 3, 5, 6, 9).

Article 9(1) permits transfer where an applicable processing condition under Article 5 or 6 and an adequacy decision are present. In the absence of an adequacy decision, Article 9(4) requires a processing condition, the data subject's ability to exercise rights and obtain effective remedies in the destination, and one of four appropriate safeguards:

- An agreement that is not an international treaty between the specified public bodies or international organisations abroad and public bodies or professional organisations with public-institution status in Türkiye, together with Board permission for the transfer (Art. 9(4)(a)).
- Board-approved binding corporate rules governing companies within a group of undertakings engaged in a joint economic activity (Art. 9(4)(b)).
- A Standard Contract published by the Board (Art. 9(4)(c)).
- A written undertaking containing provisions ensuring adequate protection, together with Board permission for the transfer (Art. 9(4)(ç)).

The available safeguard depends on the parties and the transfer relationship. Binding corporate rules concern the relevant group structure, while the public-body agreement route has its own institutional scope. Standard Contracts and written undertakings provide distinct contractual mechanisms. Where the Standard Contract route is selected, the correct controller/processor model must be used; a vendor's ordinary data-processing agreement does not itself replace the Board's published contract. Article 9(5) requires notification of the signed Standard Contract within five business days. This notification duty belongs to that route and differs from the Board permission required under Article 9(4)(a) and (ç).

Article 9(6) separately provides derogations for occasional transfers where neither adequacy nor an Article 9(4) safeguard is available. Risk-informed consent and contractual necessity have their own statutory conditions. Routine consent therefore does not provide a general basis for repetitive cloud or API transfers. Onward transfers to subprocessors must also satisfy Article 9 (Art. 9(8)).

For the venture, the consequence is that a transfer mechanism must be matched to the actual data flow and the parties' roles. A software licence or cloud subscription alone does not supply that mechanism. Conversely, a valid transfer arrangement does not settle the separate conditions governing the use of the provider's software or model.

4. Upstream software and model licences

The same external dependencies that shape a venture's data flows also determine how it may use and supply its software. A product built on third-party libraries or a downloaded model relies on the permissions granted by the relevant licences. Those permissions must be considered alongside the company's rights in its own code and the transfer arrangements discussed above, particularly where a service combines proprietary development with open-source components.

MIT, BSD and Apache 2.0 have different notice, attribution, modification and patent provisions. Apache 2.0, for example, contains its own patent grant and termination rules. The conditions attached to a particular component must therefore be identified from its actual licence. Public source code or

downloadable model weights alone do not establish an open-source licence or unrestricted commercial permission; a model's use, modification and distribution terms require their own reading.

The manner of supplying the software also matters. GPL obligations arise through the applicable licence's conveying and recipient-source provisions. AGPLv3 Section 13 additionally requires that, where the program is modified and the modified version supports remote network interaction, users interacting with it remotely are prominently offered no-charge access to that version's Corresponding Source. The scope of that source follows the licence's definitions and the technical relationship between components. An AGPL component does not automatically bring every independent part of a SaaS service within the disclosure obligation.

For the venture, the resulting question is whether its planned architecture and delivery model fit the permissions it has obtained. Serving a component only through an API, distributing copies to customers and modifying a network-interactive program can produce different licence consequences. The company can establish its authority to offer the service only by examining those uses together with its own rights chain. Regulatory obligations in the destination market remain a further question even where both are in order.

5. EU AI Act obligations for ventures established in Türkiye

Supplying an AI-enabled service to an EU customer can bring a venture established in Türkiye within the EU AI Act. Article 2(1)(a) covers providers placing AI systems or general-purpose models on the Union market, or putting AI systems into service there, regardless of their place of establishment. Article 2(1)(c) also reaches providers and deployers in third countries where the output produced by the AI system is used in the Union. A company operating from Türkiye must therefore assess its connection to the EU market and the use of its system's outputs before treating the Act as irrelevant to its product.

The company's role then determines the relevant duties. A Turkish venture supplying an AI system under its own name may be a system provider even where the product incorporates an upstream model. Merely using a model API does not itself make the company a general-purpose model provider. Changes to a system's name, intended purpose or design may also alter the allocation of provider responsibilities under Article 25. For example, a recruitment-ranking service offered to an EU customer requires an assessment of its intended use and potential high-risk classification; its Turkish place of incorporation does not resolve those questions.

These distinctions affect product design and market access. Under Article 50(1), a provider of a system intended to interact directly with natural persons must ensure that users are informed of the AI interaction, subject to the provision's conditions and exceptions. Article 50(2) addresses provider duties concerning machine-readable marking of synthetic outputs, while Article 50(4) imposes distinct disclosure duties on deployers for deepfakes and certain public-interest text. The allocation cannot be determined simply by calling the product a SaaS service: the company's role, functionality and intended use must be examined.

Representative requirements likewise depend on the role. Article 22 provides for an EU-established authorised representative for third-country providers of high-risk systems when the relevant provisions apply. Article 54 separately governs general-purpose model providers. Its paragraph 6 exempts qualifying free and open-source models that do not present systemic risk; the required licence permissions and public availability of parameters, weights, architecture and usage information must

be satisfied. Open weights alone do not establish that exemption. A Turkish system provider cannot assume that an exemption applicable to an upstream model also resolves its own system-level obligations.

The AI Act's provisions begin to apply on different dates. Chapters I and II began applying on 2 February 2025, subject to the later exceptions for specified prohibitions; general-purpose model rules began applying on 2 August 2025 subject to their transition rules. The general application date, including Article 50, is 2 August 2026. Following Regulation (EU) 2026/1744, Chapter III, Sections 1–3, except Article 6(5), applies on 2 December 2027 to Article 6(2)/Annex III systems and on 2 August 2028 to Article 6(1)/Annex I systems (Art. 113). Article 111(4) separately gives providers of synthetic-content systems placed on the market before 2 August 2026 until 2 December 2026 to comply with Article 50(2). Other existing-system and model transitions under Article 111 must be assessed for the product concerned.

For a Türkiye-based venture, those dates govern different compliance tasks. Deferral of the identified high-risk provisions does not defer an otherwise applicable Article 50 duty. The company must first establish the EU connection and its role, then identify the duties and transitional dates relevant to that role. This regulatory assessment completes, rather than replaces, the earlier analysis: rights in the code, permission to use third-party components and a lawful basis for personal-data transfers do not by themselves establish compliance with the rules governing the AI service offered to the EU market.

Relationship to earlier writing

This paper brings together and develops my earlier blog notes:

- Intellectual property, cross-border data transfers and contractual structure in AI and SaaS ventures under Turkish law.
- Open-source licence compliance and investment due diligence in software and AI projects under Turkish law.
- Extraterritorial scope of the EU Artificial Intelligence Act: implications for Türkiye-based software and AI ventures serving the EU market.

References

1. Republic of Türkiye. Law No. 5846 on Intellectual and Artistic Works, Arts. 1/B, 2 item 1 and last paragraph, 6 item 11, 18, 48, 50, 52, Additional Art. 8.
   https://www.mevzuat.gov.tr/mevzuatmetin/1.3.5846.pdf
2. Republic of Türkiye. Law No. 6698 on the Protection of Personal Data, Arts. 3, 5, 6, 9, including Law No. 7499 amendments.
   https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf
3. Personal Data Protection Authority. Cross-border transfers: adequacy decisions, appropriate safeguards and derogations under Article 9 KVKK.
   https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim
4. MIT License.
   https://opensource.org/license/mit
5. Apache License, Version 2.0, especially Sections 3–4.
   https://www.apache.org/licenses/LICENSE-2.0
6. GNU General Public License v3.0, especially Sections 5–6.
   https://www.gnu.org/licenses/gpl-3.0.html
7. GNU Affero General Public License v3.0, especially Sections 1 and 13.
   https://www.gnu.org/licenses/agpl-3.0.html
8. European Union. Regulation (EU) 2024/1689, especially Arts. 2, 22, 25, 50, 54, 111, 113; consolidated reference dated 27 July 2026.
   https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/eng
9. European Union. Regulation (EU) 2026/1744 amending the AI Act, including Arts. 111 and 113.
   https://eur-lex.europa.eu/eli/reg/2026/1744/oj

© 2026 Av. Dr. Alihan Sağır. Licensed under Creative Commons Attribution 4.0 International (CC BY 4.0). This working paper provides scholarly and general information; it is not legal advice on a particular transaction.