



De 5 meest voorkomende juridische fouten bij IT- en softwarebedrijven

Veel IT- en softwarebedrijven lopen onnodige juridische risico's. De gevolgen? Datalekken, aansprakelijkheidsclaims, verlies van intellectuele eigendomsrechten of een vastgelopen samenwerking. Deze risico's zijn meestal te voorkomen met een sterke juridische basis. In dit document behandelen we de vijf meest voorkomende juridische fouten, gebaseerd op praktijkervaring, en hoe je deze kunt vermijden.

1. Algemene voorwaarden niet op de juiste manier van toepassing verklaren

Veel bedrijven denken dat het voldoende is om algemene voorwaarden op hun website te zetten of op de factuur te vermelden. Maar juridisch gezien moeten voorwaarden voor of uiterlijk bij het sluiten van de overeenkomst ter hand worden gesteld. Als dat niet gebeurt, zijn ze juridisch niet geldig. Het gevolg is dat bij een conflict bepalingen over aansprakelijkheid, betaling of opzegging niet afdwingbaar zijn.

Voorbeelden uit de praktijk:

- Voorwaarden worden pas na ondertekening toegestuurd.
- Alleen een verwijzing op de factuur, zonder daadwerkelijke toezending.
- Geen expliciete vermelding in de offerte of e-mail.
- Klant krijgt geen toegang via een werkende hyperlink.

Zorg dus altijd voor een juridisch correcte verwijzing en levering van de voorwaarden.

- Verwijs expliciet naar de voorwaarden voor of bij het sluiten van de overeenkomst.
- Neem de verwijzing op in offerte, opdrachtbevestiging en aanmeldproces.
- Stuur de voorwaarden mee als pdf of geef toegang via een downloadbare link.
- Laat de klant actief akkoord geven (bijv. via e-mail of aanvinkvakje).
- Leg het akkoord vast in je administratie of CRM-systeem.

2. Intellectueel eigendom niet goed geregeld

Het juridisch eigendom van software of andere creaties ligt niet automatisch bij degene die ervoor betaalt. Zonder expliciete overdracht blijven de rechten bij de ontwikkelaar of freelancer. Ook founders moeten hun IE-rechten overdragen aan de vennootschap, meestal via hun managementovereenkomst. Een ander risico is dat alle IE-rechten in de werkmaatschappij zijn ondergebracht. Dat maakt je kwetsbaar bij investeringen of overnames.



Daarnaast wordt er vaak geen onderscheid gemaakt tussen broncode, content, data of documentatie, waardoor er bij geschillen onduidelijkheid ontstaat over wat er precies is overgedragen.

- Sluit met alle ontwikkelaars en freelancers een contract met expliciete IE-overdracht.
- Leg IE-overdracht ook vast in de managementovereenkomst van founders.
- Breng intellectueel eigendom onder in een aparte IP-holding voor betere bescherming.
- Maak in contracten onderscheid tussen broncode, documentatie, content en data.
- Voer een IP-audit uit bij groei, investeringen of een geplande exit.

3. Aansprakelijkheid te ruim of onduidelijk geregeld

Aansprakelijkheid is een gevoelig punt. Volledig uitsluiten mag juridisch niet. Maar als je deze te ruim of te vaag formuleert, kan dat juist leiden tot hoge schadeclaims die door de rechter worden toegewezen. Vaak wordt bijvoorbeeld alleen verwezen naar het verzekerde bedrag, of indirecte schade wordt niet uitgesloten.

Een goede beperking van aansprakelijkheid is afgestemd op je dienstverlening en verzekeringen. Zorg dat je onderscheid maakt tussen directe en indirecte schade, en dat je voorwaarden juridisch houdbaar zijn bij een rechter en duidelijk zijn voor je klant.

- Beperk aansprakelijkheid tot een redelijke hoogte, zoals 12 maanden vergoeding met een maximum van 2x dat bedrag.
- Maak geen koppeling met verzekeringsvoorwaarden, tenzij juridisch houdbaar.
- Definieer duidelijk wat directe schade is, en sluit indirecte schade expliciet uit.
- Laat je aansprakelijkheidsbepaling toetsen door een jurist met ervaring in IT-contracten.

4. Niet voldoen aan wet- en regelgeving

Softwarebedrijven hebben te maken met een groeiend aantal wettelijke verplichtingen. De AVG/GDPR geldt voor iedereen die persoonsgegevens verwerkt. Maar ook nieuwe regels zoals de NIS2-richtlijn, de AI Act en DORA zijn (indirect) van toepassing op veel IT-dienstverleners.

Bedrijven werken vaak nog met verouderde privacyverklaringen, hebben geen verwerkersovereenkomsten, en melden datalekken te laat. Ook ontbreekt vaak het beleid om beveiligingsincidenten of AI-gebruik aantoonbaar te beheersen. Dat kan leiden tot hoge boetes, reputatieschade en verlies van klantvertrouwen.

- Zorg voor een up-to-date privacyverklaring en verwerkersovereenkomsten met derden.
- Voer DPIA's uit bij risicoverwerkingen en houd een verwerkingsregister bij.
- Implementeer beveiligingsmaatregelen en incidentprocedures conform AVG en NIS2.
- Bereid je voor op AI-wetgeving met risicobeoordelingen en documentatie (AI Act).



- Zorg voor compliance bewustzijn binnen je team en leg verantwoordelijkheden vast.

5. Gebruik van templates en inkoopvoorwaarden zonder juridische controle

Veel IT- en softwarebedrijven gebruiken standaardtemplates of contracten die ze via internet of andere partijen hebben verkregen. Dat lijkt efficiënt, maar levert vaak juridische risico's op. Documenten zijn niet afgestemd op het eigen dienstverleningsmodel, bevatten verouderde bepalingen of verwijzen naar verkeerde rechtsposities.

Een SaaS-bedrijf dat bijvoorbeeld algemene voorwaarden van een softwareontwikkelaar gebruikt, loopt risico's op:

- Geen afspraken over uptime of supportniveaus
- Onduidelijkheid over IE-rechten
- Geen bepalingen over automatische verlenging of opzegging
- Gevolg: conflicten, onbruikbare documenten bij due diligence en een zwakke juridische positie bij discussies met klanten of investeerders.

Wat kun je doen?

- Gebruik alleen documenten die zijn afgestemd op jouw dienstverlening (zoals SaaS, MSP, consultancy of maatwerk).
- Laat templates of voorwaarden altijd juridisch beoordelen vóór gebruik.
- Houd rekening met actuele wetgeving (AVG, NIS2, AI Act, DORA).
- Zorg dat bepalingen over IE, aansprakelijkheid, persoonsgegevens en SLA's aansluiten bij de praktijk.

6. Inkoopvoorwaarden

Veel leveranciers accepteren zonder overleg de inkoopvoorwaarden van klanten. Dit gebeurt vooral bij grote bedrijven, multinationals en overheden, waarbij voorwaarden zoals ARBIT 2022 automatisch van toepassing worden verklaard. Die bevatten vaak een eenzijdige risicoverdeling in het nadeel van de leverancier.

- Veelvoorkomende risico's:
- Aansprakelijkheid ligt volledig bij de leverancier, vaak zonder limiet
- IE-rechten gaan automatisch over naar de klant
- Verplichtingen tot kosteloos herstel, ook bij vage klachten
- Lange betalingstermijnen (bijv. 60 dagen of meer)



Gevolg: je zit vast aan zware contractuele verplichtingen, met beperkte onderhandelingsruimte en verhoogde financiële risico's.

Wat kun je doen?

- Laat inkoopvoorwaarden altijd juridisch toetsen voor akkoord
- Wees alert op bepalingen over IE, aansprakelijkheid en herstelverplichtingen
- Stel zelf een contract of algemene voorwaarden voor ter vervanging
- Ga actief in onderhandeling over de juridische voorwaarden
- Beperk aansprakelijkheid contractueel (bijv. max. 12 maanden vergoeding met een plafond)

Samenvattend

IT- en softwarebedrijven kunnen veel juridische problemen voorkomen door hun basis op orde te hebben. Zorg voor:

- ✓ Correct toegepaste algemene voorwaarden
- ✓ Goede overdracht en bescherming van intellectueel eigendom
- ✓ Heldere en juridisch geldige aansprakelijkheidsbeperkingen
- ✓ Naleving van actuele wetgeving zoals AVG, NIS2, DORA en de AI Act
- ✓ Op maat gemaakte juridische documenten en juridische onderhandelingen met klanten

Meer weten?

Wil je jouw juridische documenten laten toetsen of heb je vragen over de onderwerpen uit dit document?

Neem dan contact op met VirtualCounsel voor een vrijblijvende afspraak:

-  Plan een videocall via www.virtualcounsel.nl of:

https://calendly.com/virtualcounsel_nl/kennismakingsgesprek-virtualcounsel

-  Stuur een e-mail naar info@virtualcounsel.nl
-  Of stuur een DM via LinkedIn

Met vriendelijke groet,

Maarten van Beek

VirtualCounsel