

Draft — pending legal review. Not yet in force.

Uprelic Acceptable Use Policy (AUP)

§ 1 Scope, purpose and how to read this Policy

1.1 Who this Policy binds. This Acceptable Use Policy applies to every use of the Uprelic service (the "**Service**") — by registered users and by users of a company workspace. Where a company workspace is concerned, the customer is responsible for compliance by all of its users. This Policy forms an integral part of the applicable Terms; a breach of it is a breach of contract.

Guests. Where you use the Service without holding an account — whether by opening a shared chat, file or artifact, by continuing a shared chat in a guest session, or by starting a chat of your own — **these rules apply to your use of the Service from the point at which they are presented to you and you accept them.** Where we ask for that acceptance, we present them before access is granted, in a form that allows you to read and store them. **Statutory duties — in particular under criminal law and under data protection law — apply to you irrespective of any acceptance,** and nothing in this paragraph limits our right to withdraw a share link or block access in order to comply with the law or to protect the Service.

1.2 What the Service can do — and why this Policy is broad. The Service does not only generate text. Its agent **acts**: it sends e-mails and messages through connected accounts, creates and deletes records in third-party systems, executes code in isolated sandboxes, retrieves and renders web pages, downloads and processes media, generates and edits images, transcribes audio, publishes content that search engines index, and runs all of this unattended on a schedule. The rules below are written against those capabilities.

1.3 You are responsible for what the Service does on your instruction. Instructing the Service to do something prohibited by this Policy is itself a breach of this Policy. It makes no difference whether the prohibited act was carried out by you directly, by the agent on your behalf, by an automation you configured, by code you had executed in a sandbox, or by a third party to whom you gave access.

1.4 Relationship to law and to third-party rules. This Policy sets contractual rules. It does not replace applicable law, the terms of the third-party services you connect, or the usage policies of the AI providers whose models the Service makes available. Where those rules are stricter, they apply in addition; how the usage policies of the AI providers bind you, and how changes to them take effect, follows from § 7.6.

1.5 Examples are examples. Where this Policy gives examples, they are illustrative and not exhaustive.

1.6 Consumers. Where you are a consumer within the meaning of **§ 13 BGB**, the mandatory provisions of German and EU consumer law apply in your favour notwithstanding anything in this Policy. **No provision of this Policy limits or excludes your statutory rights**, and in particular § 9.8 is to be read subject to §§ 249 and 309 Nr. 5 BGB, and § 9.9 only within the limits of the GDPR. Where a provision of this Policy would be invalid as against you, **the statutory rules take its place (§ 306 Abs. 2 BGB)**; the remainder of the Policy is unaffected.

§ 2 Illegal content and illegal activity

2.1 General prohibition. You must not use the Service to create, generate, store, process, distribute, publish, transmit or promote content that is unlawful, and you must not use the Service to commit, prepare, facilitate or conceal an unlawful act.

2.2 Content that is prohibited without exception. This includes in particular:

a) **Child sexual abuse material (CSAM)** and any depiction of the sexual abuse or sexual exploitation of minors, including material that is generated, edited or altered by AI (see also § 7.3); b) content that supports, glorifies, incites or facilitates **terrorism, violent extremism** or the commission of serious violent offences, and content constituting recruitment or financing for such purposes; c) incitement to hatred and violence against persons or groups, dissemination of the propaganda material or symbols of unconstitutional and terrorist organisations, and the denial or trivialisation of genocide, to the extent unlawful; d) instructions for building weapons, explosives, or chemical, biological, radiological or nuclear agents, and instructions for synthesising controlled substances; e) human trafficking, forced labour, and the exploitation of persons; f) fraud, phishing, identity theft, forged documents and identity papers, counterfeit goods, money laundering and the circumvention of sanctions; g) unlawful gambling, and the unlawful sale of regulated goods (weapons, narcotics, prescription medicines); h) infringement of third-party intellectual property rights, in particular the unlawful reproduction and distribution of protected works.

Security research, journalism, education, compliance work and defensive security work that lawfully engages with these subjects are not prohibited by this paragraph where you are entitled to carry them out; the prohibition is directed at the unlawful act and at content that is itself unlawful.

2.3 No unlawful use of the agent. You must not use connected accounts, automations, sandboxes or the browsing capability to carry out any of the acts listed in § 2.2 — for example by having the agent distribute phishing e-mails from a connected mailbox, by running an automation that publishes prohibited content on a schedule, or by having a sandbox assemble and dispatch fraudulent invoices.

2.4 Reporting and cooperation. Where we become aware of content or conduct of this kind, we may remove or block it, secure it as evidence, and report it to the competent authorities **where we are entitled or obliged to do so under the Digital Services Act (DSA) and applicable criminal law.** Where we obtain information giving rise to a suspicion of a criminal offence involving a threat to the life or the safety of a person or persons, **we promptly inform the competent law enforcement or judicial authorities and provide the relevant information available to us (Art. 18 DSA).** **We retain and disclose data in this context only to the extent permitted by data protection law and only for as long as necessary for that purpose (§ 9.9).**

§ 3 Harassment, privacy and personal rights; deepfakes; AI labelling

3.1 Harassment and abuse. You must not use the Service to harass, threaten, stalk, intimidate, defame or systematically demean persons, nor to organise or coordinate such conduct. This applies both to content published in the Service (for example forum posts and comments) and to messages the agent sends through your connected accounts.

3.2 Doxxing. You must not use the Service to compile, aggregate or publish personal data of an individual with the aim or the effect of exposing, endangering or intimidating them. This applies in particular to the compilation of home addresses, telephone numbers, workplace information, movement profiles or family circumstances from web searches, fetched web pages and connected accounts.

3.3 Personal data of others. You must not upload, ingest or process personal data of third parties without a legal basis. In particular, you must not connect an account, upload a document, or ingest a mailbox where you are not entitled to have the data it contains processed. Special categories of personal data within the meaning of **Art. 9 GDPR** (health, sexual life, political opinions, religious beliefs, trade union membership, biometric and genetic data) may only be processed where you have ensured the necessary legal basis; the Service is not designed as a system for the systematic processing of such data.

3.4 Recordings and images. Where you upload audio or video recordings, meeting recordings or transcripts to the Service, or connect a service that supplies them, you are responsible for their lawful creation and use. Recording the **non-publicly spoken word** without the consent of those speaking is a criminal offence under **§ 201 StGB**, as is the subsequent use or disclosure of such a recording; the making or transmission of **certain image recordings** is a criminal offence under **§ 201a StGB**. Obtain the consent of all participants **before** the recording is made and **before** the recording or a transcript derived from it is uploaded to or processed in the Service. The same applies to photographs and video of identifiable persons that you have analysed or edited.

3.5 No deepfakes of real people. You must not use the Service to generate, edit or distribute image, audio or video content that depicts an identifiable real person doing or saying something

they did not do or say, where this is done in order to deceive, to damage their reputation, to impersonate them, or to obtain a financial or other advantage. This includes voice cloning and the manipulation of existing recordings. Clearly recognisable satire, art and commentary that is lawful under applicable law and does not deceive as to its nature is not covered by this prohibition.

3.6 Non-consensual intimate imagery. You must not generate, edit, store or distribute intimate or sexualised depictions of a real person without that person's consent. See also § 7.3.

3.7 Impersonation. You must not impersonate another person, another company or Uprelic itself — neither through your public handle or profile, nor in content, nor in messages sent through a connected account.

3.8 AI labelling duties. Content generated by the Service is identified as AI-generated where the Service provides for this. **We will additionally mark Output in a machine-readable format as artificially generated or manipulated, in accordance with Art. 50(2) of Regulation (EU) 2024/1689 (AI Act), as amended, from the date on which that obligation applies to the Service, and in any event no later than 2 December 2026;** this does not apply where the Service performs only an assistive function for standard editing or does not substantially alter the input you supply or its semantics.

You must not remove, alter, suppress or circumvent that identification or those markings. Where you publish AI-generated content or use it vis-à-vis third parties, you must not present it as human-generated. If you use the Service to interact with your own customers, employees or other third parties, **you must disclose to those persons that they are interacting with an AI system rather than a human**, at the latest at the start of the interaction, unless this is obvious from the circumstances to a reasonably well-informed person.

Where you use Output **vis-à-vis third parties** — in particular to give advice, recommendations or decisions to your own customers, employees, patients, clients or tenants — or where you **publish** it, in the fields of **law, healthcare, insurance, finance, employment or housing**, or in academic or journalistic contexts, it must be **reviewed by a person qualified in that field before it is acted upon or published**, and the use of AI must be disclosed to the persons affected. Internal drafting, research and preparatory work that is not acted upon or published without such review is not restricted by this paragraph.

3.9 Third-party licences on Output. You are responsible for determining whether your use of Output requires a third-party licence and for complying with any such licence — in particular for generated or executed code, and for material derived from third-party sources.

§ 4 Messaging and outreach through connected accounts

This section addresses the abuse path with the highest operational risk: the Service can send e-mail and messages through the user's own connected Gmail, Slack and comparable accounts. Abuse here does not merely breach this Policy — it endangers our OAuth applications for **all** users.

4.1 No spam. You must not use the Service to send **unsolicited bulk messages**. This covers in particular:

a) mass e-mail through a **connected Gmail or other mailbox** to recipients who have not consented to receive it and with whom there is no existing business relationship permitting the contact; b) mass messages, channel invitations, direct messages or mentions through a **connected Slack workspace** or comparable messaging service, to recipients who have not consented and where no such relationship exists; c) automated outreach sequences, cold-mailing campaigns and follow-up chains built as **automations** on a schedule or webhook trigger, **where the underlying contact is not permitted under § 4.2**; d) mass comments, mentions or posts in third-party systems reached through the integration catalogue (for example issue comments, document comments, pull-request comments), where they are unsolicited or serve to advertise rather than to contribute.

Outreach and messaging that the recipient has consented to, or that is otherwise permitted under the law applicable to the contact, is a use the Service is intended for and is not prohibited by this paragraph.

4.2 Advertising e-mail and consent. Commercial communication sent through the Service must comply with applicable law on unsolicited advertising, including the requirement of prior consent where applicable, an accurate sender identification, and a functioning and easily accessible unsubscribe mechanism. You are the sender of such messages; the Service merely executes your instruction.

4.3 No evasion of recipient-side protections. You must not use the Service to circumvent spam filters, rate limits, sending quotas or blocklists of a messaging provider, for example by distributing sends across multiple connected accounts, by randomising message bodies to defeat filtering, or by rotating sender identities.

4.4 Address harvesting. You must not use the browsing, search or ingestion capabilities to build address lists for the purposes prohibited by §§ 4.1 and 4.3 (see also § 6.3).

4.5 Consequences under third-party rules. Providers of connected services may suspend your account or our application in the event of abuse. We may block the use of individual integrations, individual automations or individual accounts immediately in the event of a substantiated suspicion of abuse (§ 9), and we may be required to disclose the abuse to the affected provider.

§ 5 Security, attacks, malware and abuse of compute

5.1 No attacks. You must not use the Service to attack, disrupt, overload or gain unauthorised access to third-party systems, networks, accounts or data. This includes denial-of-service attacks, brute-force and credential-stuffing attacks, exploitation of vulnerabilities, interception of communications, and the unauthorised use of access credentials.

5.2 No scanning without authorisation. Port scans, vulnerability scans, penetration tests and comparable security testing may only be carried out against systems for which you hold **documented authorisation from the operator**, or which are your own. Security testing **against the Service itself** requires our prior consent in text form, which we will not unreasonably withhold for a coordinated test.

5.3 Malware. You must not use the Service to develop, generate, test, obfuscate, distribute or deploy malicious software, including viruses, worms, trojans, ransomware, keyloggers, botnet components, credential stealers and exploit kits. **Legitimate defensive security work — analysing samples in an isolated environment, developing detection and mitigation rules, reverse-engineering malware for defensive purposes, carrying out authorised red-team exercises, and developing exploit code within an authorised engagement or a capture-the-flag competition — is permitted where you are entitled to carry it out.**

5.4 Sandbox abuse. The code-execution sandboxes are provided for the execution of code in the context of your own work. It is prohibited to use them:

a) for **cryptocurrency mining** or comparable proof-of-work computation; b) as a **proxy, VPN, tunnel, relay or anonymisation service**, or as a mail relay; c) to host or distribute persistent services, file shares or websites; d) for distributed computation across many parallel sandboxes with the aim of obtaining compute resources beyond your plan; e) to **break out of the sandbox**, escalate privileges, attack the underlying infrastructure or other tenants, or read data of other users; f) for the storage or distribution of unlawful content.

5.5 No circumvention of resource limits. You must not circumvent the resource, run-time, concurrency or volume limits of the sandbox environment, whether by technical means or by distributing work across several accounts (see also § 8).

5.6 Our security measures. We may inspect, restrict or terminate sandboxes, automations and requests where necessary for security, abuse prevention or the protection of the Service, and we may block accounts involved in an attack with immediate effect. §§ 9.2 and 9.4 apply to such measures.

5.7 Reporting vulnerabilities; coordinated disclosure. Vulnerabilities found in the Service should be reported to **security@uprelic.com**, which is also published on our legal hub at uprelic.com/legal. You must not exploit a vulnerability beyond the extent strictly necessary to demonstrate it, and must not access, alter or exfiltrate data of other users.

We ask you to give us 90 days to remedy a reported vulnerability before publishing it, and we will endeavour to keep you informed of progress. This is a request and an intention on our part, not a contractual undertaking, and it does not restrict your statutory rights or your freedom of expression.

Safe harbour. Where you research in good faith, comply with this § 5.7 and report promptly, **we will not pursue civil claims or file a criminal complaint against you on account of the research itself**, and we will not treat it as a breach of §§ 5.1, 5.2 or 8.3.

§ 6 Web access, data collection and third-party content

6.1 You instruct the retrieval. The Service retrieves, renders, caches and analyses third-party web content, and queries an external search interface, **on your instruction**. You warrant that you are entitled to have the content in question accessed and used for your intended purpose.

6.2 Respect third-party rules. You must not instruct the Service to:

a) breach the **terms of use** of a website or online service **where that breach is unlawful or where the operator has made its objection to automated access clear** — for example by an express prohibition of automated access, by a technical access restriction, or after having asked you to stop; b) circumvent **paywalls**, registration barriers, login walls, geo-blocking or other access controls, or to use credentials you are not entitled to use for such access; c) disregard **robots directives, rate limits or other technical access restrictions** of a source in order to obtain content you are not entitled to obtain, or after that source has asked you to stop; d) infringe **copyright** or database rights in the retrieved content, in particular by reproducing or making available protected content beyond what is permitted.

Ordinary retrieval of publicly accessible pages at ordinary volumes, in order to read, summarise or analyse them for your own purposes, is a use the Service is intended for.

6.3 Data collection: unlawful or disruptive collection is prohibited. You must not use the browsing, search, ingestion or automation capabilities to collect data **where doing so is unlawful — in particular where it lacks a legal basis under the GDPR — or where it is carried out at a scale or frequency that impairs the operation of the source**. Subject to that standard, the following are prohibited in particular:

a) the systematic harvesting of **personal data** from websites, social networks, professional networks, directories or public registers, including the compilation of e-mail addresses, telephone numbers, profile data or movement data, **where it is unlawful or serves a purpose prohibited by §§ 3.2 or 4.1**; b) the **untargeted collection of facial images** or other biometric data from the internet or from CCTV footage in order to create or expand facial recognition databases — **this is prohibited absolutely**, irrespective of scale or lawfulness elsewhere, because Art. 5(1)(e) AI Act makes it so (see § 7.1(e)); c) the building of profiles of individuals from aggregated public sources **where it is unlawful, or where it serves to expose, endanger**

or intimidate the person concerned; d) the systematic replication of third-party databases, catalogues, price lists or content collections **in breach of copyright or database rights**; e) the operation of scheduled automations whose purpose or effect is continuous large-scale retrieval from third-party sites **at a scale or frequency that impairs the operation of the source**.

Research, market and competitor analysis, KYC/AML and sanctions screening, supplier due diligence, recruitment sourcing and journalistic investigation are uses the Service is intended for, and are not prohibited by this paragraph where they are lawful and conducted at ordinary volumes.

6.4 Media download (decision A3). Where the Service offers server-side download and processing of media, **you may use it only for sources that are not protected by a technical protection measure (DRM) and that you are authorised to use** — in particular your own recordings, media you have licensed, media published under a licence permitting your intended use, and media supplied from an account you have connected. **The Service does not make that assessment for you: it is yours to make before you instruct the download.**

You must not use the Service to download media protected by a technical protection measure, to circumvent such a measure (§ 95a UrhG), or to download in breach of the source platform's terms of use. We may block individual sources, or the feature, where we have a substantiated suspicion of breach.

6.5 Caching and takedown. Retrieved pages may be cached on our servers for a limited period. Rightsholders may request removal of cached content at **abuse@uprelc.com** (§ 10.1).

6.6 Attribution and onward use. Where you reproduce retrieved third-party content or Output derived from it, you are responsible for the required attribution and for compliance with the applicable licence (§ 3.9).

§ 7 AI Act: prohibited practices and excluded high-risk use

7.1 Prohibited practices. You must not use the Service for any practice prohibited under **Art. 5 of Regulation (EU) 2024/1689 (AI Act), as amended**. Contractually, and irrespective of whether the prohibition applies to you directly, the following uses are prohibited:

a) manipulative or deceptive techniques that materially distort a person's behaviour in a way that causes or is likely to cause significant harm; b) exploitation of the vulnerabilities of a person or group by reason of age, disability or a specific social or economic situation, with the same effect; c) **social scoring** — evaluating or classifying persons on the basis of their social behaviour or personal characteristics with detrimental or disproportionate consequences in unrelated contexts; d) assessing or predicting the risk of a person committing a criminal offence **solely** on the basis of profiling or of personality traits. **This does not cover the support of a human assessment that is based on objective and verifiable facts directly linked to a criminal activity**; e) **untargeted scraping of facial images** from the internet or from CCTV footage in

order to create or expand facial recognition databases; f) **emotion recognition in the workplace or in educational institutions**, save for medical or safety reasons; g) **biometric categorisation** in order to infer or deduce race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; h) **real-time remote biometric identification** in publicly accessible spaces for law enforcement purposes.

Art. 5 AI Act has been in force since **2 February 2025**. Where the AI Act as amended adds further prohibited practices, they apply from the date provided for in that amendment and are prohibited under this Policy from that date; § 7.3 is prohibited under this Policy with immediate effect.

7.2 Biometrics generally. Independently of § 7.1, you must not use the Service for **remote biometric identification of individuals in publicly accessible spaces, for building biometric databases from material you are not entitled to use, or for emotion recognition in the workplace or in educational institutions**.

7.3 AI-generated CSAM and non-consensual intimate imagery. You must not use the Service to generate, edit, store, or distribute:

a) **child sexual abuse material**, including material that is entirely artificially generated or in which an existing depiction has been altered by AI; or b) **non-consensual intimate imagery** — intimate or sexualised depictions of a real, identifiable person created or altered without that person's consent.

This prohibition applies to every generation path in the Service, including image generation and image editing, and applies irrespective of whether the person depicted exists, and irrespective of any claimed artistic, satirical or private purpose. **It is a contractual prohibition effective immediately and independent of the AI Act; the corresponding statutory prohibition was inserted into Art. 5(1) AI Act as points (ba) and (bb) by Regulation (EU) 2026/1744 and applies from the entry into force of that Regulation on 27 July 2026.** Breach of this provision leads to **immediate termination** without prior warning (§ 9.3).

7.4 High-risk and critical use. The Service is **not developed, tested, conformity-assessed or intended** for use as, or as a safety component of, a **high-risk AI system** within the meaning of **Art. 6 and Annexes I and III of Regulation (EU) 2024/1689 (AI Act), as amended**, nor for use in the operation of **critical infrastructure** (energy, water, transport, telecommunications, digital infrastructure, healthcare provision, financial market infrastructure), nor in any context in which a malfunction, an inaccurate Output or an interruption of availability could lead to **death, to injury to the life or health of a person, or to severe environmental or property damage**. Such use is prohibited.

The prohibition applies in particular where Output would be **acted upon without meaningful human oversight by a person competent to assess it and able to disregard, override or reverse it (Art. 14 AI Act)**. Examples of prohibited use include: automated decisions on recruitment, promotion or dismissal without such oversight; automated decisions on creditworthiness, insurance cover or entitlement to social benefits; use in medical diagnosis or

treatment decisions, in triage, or in the dispensing of medicines; use in the control or monitoring of vehicles, machinery, industrial plant or the supply of water, gas, heating or electricity; use in emergency call handling or in the dispatch of emergency services; use in safety components of products; and use by law enforcement, migration, asylum, border-control or judicial authorities for decisions affecting individuals.

7.5 If you use it anyway. Where you nonetheless use the Service in such a context, you do so at your own risk and on your own responsibility, you assume the corresponding provider or deployer obligations under the AI Act, and you indemnify us against the resulting third-party claims and regulatory measures in accordance with the applicable Terms. **This allocation operates between you and us; it does not affect our own obligations under the AI Act, in particular under Art. 25 AI Act.**

7.6 Provider policies. Every model the Service makes available is operated by an AI provider that publishes a usage policy of its own. **You must not instruct the Service to do, through a given model, what the provider of that model prohibits.** That is an obligation under this Policy, imposed in this Policy's own words: it does not depend on any other document forming part of your contract, and it is not affected by the status of the page named below.

We tell you which providers serve which models on the **Subprocessor and AI-provider page** at uprelic.com/legal/subprocessors; each provider publishes its own usage policy on its own site. This § 7.6 binds you only in respect of models whose provider is named on that page; where a model is served by a provider we do not name there, no provider policy binds you under this § 7.6. **That page informs you; it is not itself part of your contract.**

Where a provider changes its usage policy so as to prohibit more than it did before, the change takes effect for you only through the change procedure in § 10.3; where we are compelled to apply a changed policy sooner in order to retain access to a model, we may instead withdraw that model. The obligations in § 3.8 apply irrespective of any change to a provider policy.

§ 8 Platform integrity

8.1 No circumvention of limits and gates. You must not circumvent or attempt to circumvent the technical or contractual limits of your plan. This includes in particular:

a) circumventing **credit consumption, credit limits or top-up mechanics**, for example by manipulating requests, by exploiting metering errors, or by artificially splitting requests; b) circumventing **concurrency limits** on parallel generations, **rate limits**, file and request size limits, or the limit on **active scheduled automations**; c) creating or using **multiple accounts** in order to obtain repeated free allowances, to evade a block, or to distribute usage in excess of your plan; d) sharing an account or a seat between several persons, or rotating a seat systematically in order to serve more persons than seats booked; e) circumventing **feature gates** for functionality not included in your plan.

8.2 No resale of access. You must not resell, rent, lease, share or otherwise make access to the Service available to third parties, and must not operate a service based on the Service for third parties, unless expressly agreed with us in text form.

8.3 No reverse engineering. You must not reverse engineer, decompile or disassemble the Service, or attempt to derive its source code, system prompts, model weights, internal architecture or non-public interfaces — including by prompt-based extraction attempts directed at obtaining system instructions or internal configuration. **Mandatory statutory permissions, in particular §§ 69d and 69e UrhG, remain unaffected, as does good-faith security research under § 5.7.**

8.4 No scraping of the Service. You must not scrape, systematically retrieve, index or mirror the Service, its public content or its interfaces, whether by script, headless browser or otherwise, save with our prior consent in text form — this does not apply to the indexing of our public pages by general-purpose search engines in accordance with the directives we publish at `/robots.txt`.

8.5 No training of competing models on Output. You must not use Output, or data derived from it, to **develop, train, fine-tune, distil or improve a competing AI model, AI system or competing service**, nor to build a dataset for that purpose.

Publishing a benchmark or comparison of the Service is permitted, provided that you state the models, plan and date tested, describe your method, and do not present the results as ours. *(Business customers: the Business Terms § 7.3(c) additionally require our prior written consent for benchmark publication; that stricter rule applies only to customers under those Terms.)*

8.6 No interference with the Service. You must not use the Service in a way that impairs its operation or its use by other users to a more than insignificant extent, in particular through automated mass requests, artificially generated load, or the deliberate triggering of error states.

8.7 No falsification of identity or telemetry. You must not falsify metadata, identifiers, timestamps or telemetry, and must not disguise the origin of requests in order to evade our abuse prevention.

§ 9 Enforcement — and how we moderate content

This section is also our disclosure under **Art. 14(1) DSA**: it sets out the restrictions we impose in respect of the content of the recipients of our service, and the policies, procedures, measures and tools we use for content moderation, including algorithmic decision-making and human review. It is addressed to **all recipients of the service**, including users of a company workspace and guests, and it is published at a stable public address in a machine-readable format.

9.1 Graduated measures. Where we have a substantiated suspicion of a breach of this Policy, we may take one or more of the following measures, choosing the mildest measure that is effective in the circumstances:

Step	Measure
1	Warning with a request to remedy the breach within a set period
2	Throttling or restriction of individual functionality — for example blocking a specific integration, an automation, sandbox use or the browsing capability; reducing rate and concurrency limits
3	Removal or blocking of content , restriction of its visibility, removal from search-engine indexing
4	Suspension of the account, of individual users, or of the workspace
5	Termination for good cause and permanent exclusion from the Service

The statutory requirements for termination, in particular § 314 Abs. 2 and § 543 BGB, remain unaffected, as do your statutory rights arising from a measure that turns out to be unjustified.

9.2 Proportionality and fundamental rights. Which measure we take depends in particular on the seriousness of the breach, whether it was repeated, the degree of fault, the harm caused or threatened, and the interests of the persons affected. Measures are limited in scope and duration to what is necessary. **We apply them diligently, objectively and proportionately, with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service as enshrined in the Charter of Fundamental Rights of the European Union (Art. 14(4) DSA).**

9.3 Immediate measures without warning. We may skip steps 1 and 2 and act immediately — including permanent exclusion — where the breach is serious, in particular in the cases of § 2.2(a) and (b) and § 7.3, in the event of attacks on the Service or on third-party systems (§ 5), where immediate action is necessary to avert a serious risk, or where an authority or a court so requires. § 9.4 applies to such measures in the same way.

9.4 Statement of reasons (Art. 17 DSA). Where we remove content, restrict its visibility, restrict monetisation, or suspend or terminate an account, we provide the affected recipient of the service with a **clear and specific statement of reasons, at the latest at the time the restriction takes effect**, containing at least:

a) the measure taken, and its territorial scope and duration; b) **the facts and circumstances on which the decision is based, including whether the decision was taken on the basis of a notice submitted under Art. 16 DSA or on our own initiative, and, where strictly necessary, the identity of the notifier**; c) whether **automated means** were used in detecting

the content and in taking the decision; d) the contractual or legal ground relied on, and an explanation of why the content or conduct is incompatible with it; and e) information on the available means of redress, in particular under § 9.6.

This does not apply to orders under Art. 9 DSA (Art. 17(5) DSA), or where the content concerned is deceptive high-volume commercial content (Art. 17(2) DSA); and it applies only where we know the electronic contact details of the recipient concerned (Art. 17(2) DSA).

9.5 How we detect breaches; automated first pass and human review. We act on the basis of (i) reports under § 10.1, (ii) orders from authorities and courts, (iii) our own checks, and (iv) **automated systems** — in particular the automated filters of the AI providers and our rate limits. **Automated systems can produce errors.**

Potential breaches are detected in a **first pass by automated systems**, and measures taken on the basis of such a signal **may take effect without prior individual review by a human being**. A measure to which § 9.4 applies is accompanied by a statement of reasons under that clause; every measure can be challenged under § 9.6. **Where you object, the decision is reviewed by a natural person, and we inform you of the outcome.**

9.6 Objection. You may object to a measure at appeals@uprelic.com. We re-examine the decision, have it reviewed by a natural person, and inform you of the outcome with reasons. Recourse to the courts, and — where applicable — to a competent out-of-court dispute settlement body under the DSA, remains unaffected.

9.7 Repeat infringers. Users who repeatedly publish manifestly illegal content or repeatedly breach this Policy despite warning may be excluded from the affected functionality for a reasonable period, and in serious cases permanently.

9.8 Cost recovery and damages. You must reimburse us the costs **reasonably and actually** incurred as a result of a breach of this Policy for which you are responsible, in particular the costs of remedial and recovery measures and of legal defence against third-party claims, **in each case only to the extent recoverable under § 249 BGB. You are entitled to show that no cost, or a lower cost, was incurred.** Statutory claims for damages, the indemnity provisions of the applicable Terms, and our right to terminate for good cause remain unaffected. **Credits consumed by usage in breach of this Policy are not refunded; your statutory claims in respect of credits consumed through a measure that turns out to be unjustified are unaffected.**

9.9 Preservation and disclosure. We may retain data relating to a breach **for as long as, and only to the extent, necessary** to investigate it, to defend against claims, or to comply with a statutory or official obligation, **and only where a legal basis under the GDPR applies.** We may disclose such data to authorities and to affected third-party providers **where we are entitled or obliged to do so**; we inform you of a disclosure where we are permitted to do so.

§ 10 Reporting, contact and changes to this Policy

10.1 Reporting a breach or illegal content (Art. 16 DSA). Breaches of this Policy, and content you consider illegal, can be reported at any time by e-mail to **abuse@uprelic.com**. No account and no login is required, and you may write in German or in English. A report should describe the content or conduct, state its exact location (URL), explain why you consider it unlawful or in breach of this Policy, give your name and e-mail address (except for reports concerning offences against sexual self-determination), and confirm your good-faith belief that the information is accurate and complete.

We confirm receipt to you without undue delay. We process reports and decide in a timely, diligent, non-arbitrary and objective manner (Art. 16(6) DSA), inform you of our decision and of the possibilities of redress against it, and tell you whether automated means were used in handling your report.

10.2 Points of contact. Our point of contact for authorities, the Commission and the Board (**Art. 11 DSA**) and our point of contact for recipients of the service (**Art. 12 DSA**) is **info@uprelic.com**. The languages accepted are **German and English**. Both contact points are also published at uprelic.com/legal/dsa and in the applicable Terms.

10.3 Changes to this Policy. We may amend this Policy in accordance with the change procedure set out in the applicable Terms, in particular in order to reflect changes in the law, new functionality, or new requirements imposed by AI providers or third-party services. **We notify significant changes in advance, present them, and draw attention to your right to object and to the consequences of not objecting.** Every version of this Policy carries a **version number and a date** and remains retrievable via the version selection on this Policy's page, each version at its own permanent address. **The version that binds you is the version in effect for you under that procedure, not whichever text happens to be published at this address at a given moment.**

10.4 Contact and provider.

Uprelic GmbH Liebenwalder Straße 16, 13347 Berlin, Germany Registergericht: Amtsgericht Berlin (Charlottenburg), **HRB 288877 B** Geschäftsführer: Marco Herzog E-Mail: info@uprelic.com

Purpose	Address
General enquiries	info@uprelic.com
Reports of illegal content and breaches of this Policy	abuse@uprelic.com
Objections to a measure (§ 9.6)	appeals@uprelic.com
Security vulnerabilities, account compromise	security@uprelic.com
Data protection	privacy@uprelic.com

Purpose	Address
DSA points of contact (Art. 11, 12)	info@uprelic.com