UNVERZAGT
RECHTSANWÄLTE

Memorandum

to: ENFORCE Consortium

from: Dr. Lukas Mezger, UNVERZAGT Rechtsanwälte

date: 20 July 2026

re: **Compliance requirements for citizen scientists conducting field work and reporting environmental violations**

I. Questions presented

The ENFORCE project engages in citizen science activities in which non-professional citizens are encouraged to contribute to environmental compliance through the collection and, where appropriate, analysis of environmental data in accordance with scientifically established methodologies and protocols.

Environmental information generated through these citizen science activities is submitted to a central database, the ENFORCE Data Plaza, where datasets are aggregated and scientifically validated. The database is intended to support the monitoring of environmental compliance, the identification and documentation of potential environmental violations, and the provision of validated environmental datasets for regulatory, policy, and enforcement purposes. Where appropriate, such datasets may also support evidentiary submissions in administrative and judicial proceedings.

Through the ENFORCE Data Plaza, the project addresses not only the supply side of citizen generated data (that is, the flow of data from citizens to authorities) but also engages with the demand side of environmental compliance, targeting the needs of environmental compliance authorities in terms of data inputs from civil society. For example expert interviews brought in demand-side perspectives regarding the barriers, opportunities and practical conditions for us-

ing citizen-generated data in compliance-related procedures.[1] Also, guidance material addresses both the supply side and the demand side of compliance assurance delivering guides, addressed to both to citizens and to prosecutors aimed to support citizen science communities in understanding how data should be collected, documented and communicated, while also helping prosecutors and legal professionals consider how such evidence may be assessed and used.[2] The initiative focuses on biodiversity conservation, forest governance and logging activities, and pollution control.

Against this background, the following questions are presented:

1. Which conditions must be met for a citizen scientist to lawfully access land to conduct field work?
2. Under which circumstances can a citizen scientist take photos or record videos depicting other people or vehicles, or otherwise document personal data?
3. When is it permissible to publish images or information containing personal information?
4. Which requirements must be met when integrating data from federated databases into a central database, particularly regarding intellectual property and privacy and who is liable for their legality?

[1] Project deliverable D2.1 ("Environmental Compliance: A Review", soon available on https://join-enforce.eu/library/ and on https://zenodo.org/communities/enforceproject/records.
[2] Developed under project task 2.1, coordinated by project partner UTH.

II. Brief answer

1. Data Collection

Physical access to land or facilities is only permissible where no restrictions are apparent or where explicit consent has been obtained. Fenced, gated, or otherwise restricted areas must not be entered without prior authorisation.

Ecologically sensitive areas are subject to layered protection regimes. Access is generally allowed only where compatible with specific site regulations, which may impose spatial or seasonal restrictions or prohibit entry entirely. The entry to military and security-sensitive sites is only lawful with prior written authorisation from the competent authority.

Field work must comply with all applicable environmental and nature conservation regulations. This includes avoiding disturbance to protected species and habitats, refraining from unauthorised sampling or removal of biological material, and ensuring that any intervention (including installations or repeated site visits) is legally permitted. Particular rules apply during sensitive (e.g. breeding or migration) periods. It must be ensured that no invasive species are released. Imports, exports, and transit of animals or plants must be declared at customs.

2. Image and Personal Data Handling

Photographs and videos that allow identification of individuals or vehicles constitute personal data under EU privacy law.[3]

Such data may only be processed on a valid legal basis, specifically adequate legitimate scientific and conservation interests. Where ENFORCE and its affiliated citizen scientists act to

[3] Art. 4(1) GDPR.

conduct scientific field work, document environmental harm, and inform the scientific community, the authorities, or the public, processing may, in certain cases, fall under the so-called journalism exception,[4] allowing for a more flexible balancing of rights. Nevertheless, the collection and subsequent processing of personal data must meet data minimisation and proportionality requirements.

As a rule, individuals should not be identifiable in published material unless there is a clear and overriding public interest. Faces and other identifiers should be blurred by default. Internal collection of personal data must also be strictly limited to what is necessary for documentation and verification purposes.

3. Publication of Information

The publication of images and information involving identifiable individuals also triggers privacy requirements.

Consent is generally required for publication of personal data unless certain exceptions apply. However, these exceptions do not provide for a general privilege for scientific research or public-interest reporting, unless publishing the personal data in question is critical for the underlying legitimate purpose.

Even where publication of personal data is permitted, ENFORCE and its affiliated citizen scientists must ensure that the content does not disproportionately affect the privacy of the depicted individuals. Images should only depict individuals if necessary to document e.g. threats to the environment, or systemic issues. A case-by-case balancing of the public (scientific and environmental) interests and the individual privacy rights is always required, particularly where there is a risk of reputational damage.

[4] Art. 85 GDPR.

4. Data Aggregation

The creation of consolidated databases combining data from multiple sources touches on both intellectual property and privacy.

The aggregation of third-party data and publications is only lawful where the necessary rights are secured (e.g. through (open) licences which may require e.g. attribution and non-modification). Any structural or textual reuse must comply with the licence terms of the data source.

Where personal data is included in the published information, aggregation requires a corresponding legal basis (either consent or legitimate interests). Depending on the context, special privileges may apply insofar as the database serves scientific and environmental protection purposes.[5]

In general, the inclusion of external data should follow a structured approach: including (sensitive) personal data, requires a (strong) justification. Where possible, reliance should therefore be placed on datasets that have already undergone legal vetting at the source.

III. Facts

This memorandum is designed to equip ENFORCE project partners with a clear and practical understanding of the legal framework within which they operate. By identifying both risks and potential mitigation strategies under European law, it aims to enable the project to pursue its mission to investigate, document, aggregate, and publish information on environmental harm, unlawful pollution, biodiversity loss and related misconduct in a central database as effectively and confidently as possible.

[5] Art. 85 GDPR.

Projects that aim to expose misconduct and thereby contribute to the protection of the environment such as ENFORCE increasingly fulfil the role of “public watchdogs,” contributing to transparency in matters of significant public interest. The European legal systems recognize and protect such activities, particularly through fundamental rights such as freedom of expression (including the freedom of the press), freedom of science and freedom of information. In addition, environmental protection as a constitutional objective may also play a role in justifying the protection of such activities. At the same time, these activities take place within a structured legal environment that imposes obligations and limits, especially in the areas of criminal law, privacy and intellectual property.

Against this backdrop, this memorandum outlines the key legal parameters governing the project’s work across three core stages:

– the collection of data and information;

– the publication and dissemination of this data and resulting research;

– the aggregation and structuring of data in national or EU-wide databases.

Rather than merely highlighting constraints, the memorandum seeks to clarify the scope of lawful action and to identify strategies for operating securely within these boundaries. It also examines potential legal justifications and defences available when the organization acts in pursuit of environmental protection and in the public interest. In doing so, it provides a foundation for informed decision-making, helping the project minimise its legal exposure while maximising the impact and reach of its activities.

IV. Applicable Law

The relevant applicable laws include the General Data Protection Regulation (GDPR) insofar as personal data are processed during environmental research and the documentation of possible violations. This includes photographs, video recordings, and other information that allow

the identification of natural persons.[6] In addition, national laws protecting personality rights may apply and ensure the protection of individuals' privacy, dignity, and reputation, particularly in connection with the publication of information and visual material.

Furthermore, copyright law provisions apply, especially regarding the use, adaptation, and publication of images, video material, and other data, as well as the reuse of external datasets.

Criminal law provisions and administrative regulations also apply, including in cases involving unauthorised access to property, unlawful handling of data, or the dissemination of sensitive information.

Finally, applicable national and EU environmental and nature conservation laws must be considered, defining the legal framework for access to protected areas, the handling of protected species and habitats, and the conducting of field research.

V. Legal evaluation

1. Data Collection

(a) Physical Access and Trespassing

A central legal risk in environmental field research arises where citizen scientists physically enter non-public land or premises to collect data.

(aa) Access to private or restricted property

Researchers and activists must limit their site visits and documentation on areas that are openly accessible and not subject to access restrictions unless prior authorisation has been granted.

[6] Art. 4(1) GDPR.

Areas that are fenced, walled, gated, locked, or marked with signs indicating restricted access are not freely accessible. In such cases, entry is only permitted with the consent of the person responsible for the site, such as the owner, tenant, operator, or other authorised possessor.[7] Where these indicators are present, researchers must seek permission in advance before entering.

If a site is not enclosed and shows no clear signs of access restrictions, entry is permitted.

A practical approach is to prioritise transparency and caution: when in doubt, seek permission, focus on clearly accessible areas, and document from public or open vantage points, where possible.

(bb) Access to bio-sensitive locations

Generally, individuals enjoy a right to enter the open landscape, reflecting the idea that nature should be accessible. However, this right is not absolute. Where areas are designated as protected sites, such as nature reserves, national parks, or biosphere reserves, entry is restricted to the extent defined by the applicable protection regulations. Entry is prohibited where these regulations exclude public access altogether.

Protection regulations frequently allow access for the general public under defined conditions, including requirements to stay on marked paths, observe seasonal restrictions, or avoid designated sensitive zones. Where no specific rule exists, movement by bicycle is often limited to roads and suitable paths.

European law does not establish uniform access rules for all protected areas. It provides a general structure that is specified by national and regional legislation and individual protection ordinances. These determine whether access is freely permitted, restricted to designated

[7] TK-StGB/Sternberg-Lieben/Schittenhelm, 31. Aufl. 2025, StGB § 123 Rn. 16.

routes, limited in time, or fully excluded in specific zones. As a result, the legality of entering a specific area depends less on its general classification and more on the specific rules applicable at that exact location.

This means that ideally, researchers and activists need to verify in advance whether any laws or protection ordinances impose access restrictions on the area they want to survey. Where access restrictions exist or where the legal situation is unclear, prior authorisation from the competent authority is required before entry.

(cc) Access to military-sensitive locations

Environmental researchers may have legitimate scientific reasons to access military areas to conduct biodiversity assessments, ecological monitoring, or environmental sampling. However, access to such sites is never granted by default.

Military installations, training grounds, and other defence-related properties are generally restricted. They are closed or controlled for security and operational reasons. Entering such areas without prior authorisation is unlawful, even if the purpose is scientific and no damage is intended.

Lawful access is only possible with prior explicit permission from the military authority responsible for the site. In practice, this usually involves a formal application process submitted in advance, clearly describing the purpose of the research, the exact locations, methods, timing, and duration of fieldwork. Authorisation is granted on a case-by-case basis and may include strict conditions such as restricted access zones, time limitations, escort requirements, or additional safety and security measures.

ENFORCE partners must ensure that no entry into any military area is undertaken without confirmed written approval from the relevant authority in the respective country.

(b) Environmental Fieldwork and Sampling

When carrying out environmental investigations, field research, sampling, or monitoring activities in natural areas, ENFORCE partners must ensure that operational methods are designed to avoid interference with protected species, habitats, and conservation areas.

European nature conservation laws generally allow the observation and documentation of nature. The collection and appropriation of wild-growing flowers, grasses, ferns, mosses, lichens, fruits, mushrooms, teas, and medicinal herbs, as well as branches of wild plants from nature is limited to locations that are not subject to a prohibition on entry, provided that it is carried out in small quantities and solely for personal use.

Limits are imposed where investigative activities disturb ecosystems, damage habitats, or involve the collection or transport of biological material. Field activities must not involve the pursuit, capture, injury, or killing of wild animals of strictly protected species, nor the removal, damage, or destruction of their developmental stages. The same prohibition applies to wild plants of strictly protected species. Strictly protected species include all animal and plant species designated under national law, European bird species, as well as species listed in the relevant European conservation regulations and directives.[8] The removal, damage, or destruction of wild plants of strictly protected species, including their developmental forms or habitats, may fall under an exception for purposes of research, teaching, education, or reintroduction, as well as related measures of breeding or artificial propagation. In such cases, however, a prior authorisation issued by the competent authority is usually required.

[8] Cf. Annexes A and B of Council Regulation (EC) No 338/97 and Annex IV of Directive 92/43/EEC.

For wild animals and plants that are not classified as strictly or specially protected species, the disturbance, capture, injury, or killing of wild animals without reasonable cause is prohibited, as is the removal or use of wild plants cause and the destruction or significant impairment of their populations or habitats. A reasonable cause exists where the actions are carried out for scientific or nature-related investigations.

Any activity that causes disturbance during sensitive periods such as breeding, nesting, rearing, moulting, migration, or hibernation is unlawful. A disturbance is legally relevant where it worsens the conservation status of a local population.

Citizen scientists must also ensure that no invasive species[9] are introduced, spread, bred, or transported during field operations. Therefore, equipment, footwear, vehicles, and sampling tools must be cleaned and handled carefully to prevent unintentional transfer of relevant organisms between sites.

All imports, exports, and transit movements of animals or plants subject to trade controls must be declared at customs.

In general, research activities should avoid causing direct or indirect environmental harm. This includes damaging vegetation, burning ground cover, cutting trees, hedges, reeds, or shrubs during protected seasons, or interfering with ditches, water bodies, or sensitive biotopes.

In practice, citizen scientists may carry out robust and lawful environmental investigations in nature by applying a ‘minimum impact’ approach: remain on public paths where possible, use non-invasive observation techniques, when possible, avoid sensitive periods and protected

[9] Invasive species are those included on the regularly updated Union list; cf. https://bfn.bsz-bw.de/frontdoor/deliver/index/docId/1133/file/Schrift654.pdf.

habitats, and obtain permits where sampling or installations are necessary in restricted nature areas, private property, or military grounds.

(c) Taking Photographs and Videos

When documenting environmental harm, citizen scientists may rely on photographs as an important evidentiary and communication tool. However, capturing images of individuals that allow for identification constitutes processing of personal data.[10] Generally, such processing requires a legal basis, such as consent or a legitimate interest.[11]

At the same time, European law recognizes that activities aimed at informing the public about matters of significant public interest such as environmental harm and unlawful pollution deserve protection. Under EU privacy law, most data protection rules do not apply where processing is carried out for journalistic purposes.[12] Processing personal data is considered 'journalistic' where its purpose is to disseminate information, opinions, or ideas to the public, and where publication is intended for an indeterminate group of recipients. This concept is interpreted broadly and covers all stages of data processing, from collection to dissemination. It even extends to the publication of unlawfully obtained information, provided that the dissemination does not disproportionately infringe the personality rights of the individuals concerned and contributes to public debate.[13]

[10] Art. 4(2) GDPR.
[11] Art. 6(1) GDPR.
[12] Art. 85(1) GDPR.
[13] Paal/Pauly/Pauly, 4. Aufl. 2026, VO (EU) 2016/679 Art. 85 Rn. 8.

For citizen scientists, this means that where they document and publish environmental violations to inform the public and promote accountability, they can rely on this broader understanding of journalistic activity and benefit from a degree of flexibility under data protection law such that a separate legal basis is not required.

However, the collection of images and video material still interferes with individual personality rights, even where data protection rules do not apply as such. Such interference is not automatically unlawful. It becomes legally relevant only where it is not justified by competing constitutional rights, in particular the freedoms of the press and scientific freedom, which must outweigh the interference with personality rights in the specific case.

This requires a structured balancing of interests: First, the severity of the interference with personality rights is assessed. Second, the weight of the freedoms of the press and science is determined. The collection is permissible where the freedoms of the press and science carry greater weight than the interference with personality rights.

The severity of any interference with personality rights depends primarily on the level of identifiability and the proximity of the information to the private sphere. Interference is limited where individuals are not recognisable or are only incidentally captured in a wider context. It increases where faces or other identifying features constitute the main focus of the image or recording, or where images or recordings reveal private or sensitive aspects of a person’s life. Also, recording without publication affects personality rights to a lesser extent than publication.

The weight of the freedoms of the press and science depends on the purpose and relevance of the documentation. It increases where the environmental harm, pollution, or unlawful conduct is of such significance that it is of strong public interest.

Where images and video material are collected solely for the purpose of documenting environmental harm in the public interest, and where individuals are only incidentally affected without disclosure of sensitive information, the freedoms of information and science generally prevail. In such cases, the collection of images is legally unproblematic.

(d) Recording of Other Personal Data

The same considerations apply to the collection and internal documentation of personal data beyond photographic or video material. This includes, for example, the recording of names, addresses, license plates or other identifiers that can be linked to an identifiable individual.

Such information also constitutes personal data[14] when it relates to an identified or identifiable natural person. Accordingly, its collection and storage for internal purposes must likewise be based on a valid legal basis,[15] such as legitimate interests where the documentation of environmental harm requires the structured recording of relevant facts.

Where such data is collected only for internal use in the context of documenting and researching environmental harm, the same principle applies as for visual material: activities aimed at identifying, recording, and structuring information relevant to public-interest environmental issues fall within a broader understanding of information-gathering activities and are considered 'journalistic'. Therefore, a separate legal basis under privacy law[16] is not required.

Just as with the taking of images and recording video, the collection and recording of other personal information interferes with personality rights as well but is not unlawful where it is justified by the freedoms of information and science. The principles set out above apply ac-

[14] Art. 4(1) GDPR.
[15] Art. 6(1) GDPR.
[16] Art. 6(1) GDPR.

cordingly. Generally, where information is collected for the purpose of documenting environmental conditions or environmental harm in the public interest and where it only affects individuals to a limited extent, the freedoms of information and science prevail over the right to privacy.

(e) Possible justifications in exceptional situations

Under certain circumstances, activities that would otherwise not comply with the principles outlined above may nevertheless be justified under the legal state of emergency. This type of justification requires (1) a present or imminent danger, (2) the suitability and (3) necessity of the citizen scientist's actions to avert that danger, and (4) a balancing of interests in which the protected interest clearly outweighs the competing legal interests.[17] However, the legal threshold for such a justification is high and must be applied restrictively.

A key requirement is the existence of a present or imminent danger, meaning a situation in which harm is highly likely to occur in the near future. In an environmental context, this underlying danger is understood by some legal scholars in a broader sense in light of the progressing climate crisis and its cumulative impacts on ecosystems and human health.[18]

In addition, any action taken under this exception must be suitable and necessary to avert that danger. An action is suitable only where it addresses a concrete and identifiable risk situation.[19] This is the case where a clearly imminent harm can be demonstrated, such as the imminent clearing of a forest, large-scale unlawful hazardous emissions or discharges, or immediate serious threats to protected habitats or water resources. Besides, the suitability requirement stipulates that the action taken must contribute (directly or indirectly) to the prevention of

[17] See e.g. sec. 34 German Criminal Code.
[18] Schmidt, Der „Klimanotstand" als rechtfertigender Notstand?, KlimR 2023, 16.
[19] Schmidt, Der „Klimanotstand" als rechtfertigender Notstand?, KlimR 2023, 16.

harm.[20] For example, documentation may be considered suitable if it can create or sufficiently raise public awareness to influence competent third parties and thereby help prevent or mitigate environmental damage.

However, the additional necessity requirement sets a stricter limit. The action must be the least intrusive means available. Where alternative, equally effective but less intrusive options exist, such as calling the competent authorities, initiating legal proceedings, or using public advocacy tools (e.g. protests or political processes) this requirement will not be met.[21]

Finally, a balancing of interests must clearly favour the protection of the threatened interest over the interference caused by the measure.

In practice, these conditions are difficult to satisfy in full in individual cases, and their assessment depends heavily on the specific circumstances of each case. Citizen scientists should therefore treat such situations as exceptional and, where possible, seek legal guidance before relying on this type of justification.

2. Data publication

(a) Publication of photographs

As described above, EU privacy law does not apply where the publication of photographs is carried out for journalistic purposes.[22] However, the publication and dissemination of identifiable images is additionally subject to personality rights regimes under national law which apply independently.[23]

[20] AG Flensburg, Urt. v. 06.12.22, Az. 440 Cs 107 Js 7252/22.
[21] OLG Celle BeckRS 2022, 21494 Rn. 7.
[22] Art. 85(1) GDPR.
[23] Loewenheim UrhR-HdB/Schertz, 3. Aufl. 2021, § 18 Rn. 6; OLG Köln, Beschluss vom 18.6.2018 – 15 W 27/18.

Images of identifiable individuals may thus only be disseminated when consent is given or when a legally recognised exception applies. In contrast to the exemption under EU privacy law for journalistic activities, these national personality rights regimes do not provide a comparable exemption for the publication of photographs and videos for journalistic purposes. Accordingly, reporting in the public interest does not automatically justify the publication of images depicting identifiable individuals.[24]

Identifiability is interpreted broadly and arises not only from facial features but also from contextual elements such as clothing, posture, location, or associated objects like vehicles.

The publication of images showing individuals without consent requires that the depicted persons are either not identifiable, that the images are taken in the context of public or collective situations,[25] or that the focus of the image clearly lies on environmental conditions, impacts, or potential misconduct rather than on specific individuals.[26] This can be achieved, for example, by documenting broader scenes in which individuals appear only incidentally as part of the surrounding environment or location.

In all cases, the publication of photographs must not result in a disproportionate interference with a depicted person's private life, reputation, or the risk of misleading portrayal.[27] The available jurisprudence emphasises that the threshold for such reputational relevance is interpreted broadly. It is not limited to unlawful or immoral conduct but extends to any image-based representation that is capable of substantially influencing how a person is perceived in society. Courts generally do not require evidence of actual reputational harm. It is sufficient that the

[24] Loewenheim UrhR-HdB/Schertz, 3. Aufl. 2021, § 18 Rn. 114.
[25] § 23 Abs. 1 Nr. 3 KUG.
[26] § 23 Abs. 1 Nr. 2 KUG.
[27] § 23 Abs. 2 KUG.

image is objectively capable of causing such an impairment. This also includes images documenting individuals allegedly engaging in unlawful conduct, where the mere dissemination of the visual impression may affect public perception regardless of whether the alleged conduct is ultimately confirmed.

Therefore, citizen scientists must avoid any disproportionate interference with private life, reputational harm or misleading portrayal of the individuals concerned. Where identifiability cannot be avoided and the legal assessment remains uncertain, practical safeguards such as subsequent anonymization, obtaining consent, or seeking legal clarification whether sufficient legitimate scientific interests warrant the publications of photographs depicting individuals.

(b) Publication of other personal data

Also regarding this type of data, EU privacy law does not apply where processing is carried out for journalistic purposes.[28] However, the publication of personal information still constitutes an interference with personality rights under national legal regimes, which applies independently of EU privacy law.

Publishing personal data constitutes a more severe interference with individuals' privacy than the mere collection or internal documentation of information, in particular where individuals are identifiable and where publication links them to alleged criminal conduct, or environmental harm. To be clear, such interference is not automatically unlawful. Again, it must be assessed on the basis of the balancing of principles set out above, which apply accordingly.

As a general rule, publication personal information is only justified where the freedoms of information and science outweigh the interference with personality rights, taking into account the

[28] Art. 85(1) GDPR.

increased impact of public attribution and the need for careful assessment of the relevance of the information to matters of significant public interest.

3. Data aggregation

When consolidating data from multiple national databases into a single uniform international database such as *ENFORCE Data Plaza*, several legal frameworks must be considered.

(a) Intellectual property aspects

From an intellectual property perspective, the reuse of textual or structured content is generally only permissible where the publishing organisation is either the original author of the material, has obtained the necessary transfer of rights from the respective authors, or has secured an appropriate licence. In many cases, source databases operate under standard open licences, which permit redistribution provided that e.g. proper attribution to the original author is given and/or that no derivative or modified versions of the original text are created. In such a case, this would require a word-for-word transfer of the source material without editorial adaptation.

(b) Data privacy aspects

Where the transferred data includes personal data, the compilation of such a database constitutes a data processing activity requiring a valid legal basis. At the same time, where the purpose of the database is to inform the public or support transparency and accountability, an exemption or limitation may apply under the journalistic or public-interest balancing framework recognised under EU or national law.

In practice, this then requires a balancing of interests: the sensitivity of the personal data and the associated impact on the rights and freedoms of data subjects must be weighed against the strength of the public information interest. As a general rule, the more sensitive the data, the higher the threshold for inclusion, and the greater the need for restraint. Where possible, it

is advisable to rely on data that has already undergone a proper review at the level of the original federated databases, thereby allowing for structured and consistent reuse, while still ensuring compliance with applicable legal standards.

(c) Liability for user generated content

The extent of ENFORCE's responsibility for verifying and moderating environmental allegations published by users (e.g., claims that an individual or company is polluting the environment) depends primarily on its role in relation to the content and the degree of control it exercises over its publication.

As a general principle, platforms are typically liable only for their own content or for third-party content that can be attributed to them as their own. Such attribution requires more than the mere provision of a neutral technical hosting environment. Instead, it is necessary that the platform either expressly assumes responsibility for the content or, assessed from the perspective of a reasonable average user and in light of all relevant circumstances, creates the impression that it endorses or identifies with the information.[29]

The likelihood of content being attributed to the platform increases where the platform engages in editorial activities such as reviewing, selecting, editing, or curating user-generated content. In particular, any form of substantive intervention may contribute to a perception that the platform has assumed responsibility for the content. In this context, even limited review activities, including checks for completeness or plausibility, may be relevant indicators of such adoption.[30]

[29] MüKoBGB/Wagner, 9. Aufl. 2024, § 823 Rn. 943.
[30] MüKoBGB/Wagner, 9. Aufl. 2024, § 823 Rn. 943, 984.

Conversely, where a platform limits its role to the passive hosting and neutral transmission of user-generated content, and clearly distinguishes such content from its own, it will generally not be considered responsible for the accuracy or legality of user statements. This position is reinforced where the platform avoids presenting user content under its own branding and refrains from exerting editorial control over its substance.[31]

[31] Auer-Reinsdorff/Conrad/Sobola, IT- und DatenschutzR-HdB, 3. Aufl. 2019, § 42 Rn. 17.