

Document Type	Policy
Document Name	Whistleblowing Policy
Effective as of	01/08/2023
Last Updated	02/02/2024
Version	V2
Created by	Lydia Kothmeier, Marisa Alves Pereira <b>and reviewed by</b> Amarilda Ulrich, Cristina San Martin, Clemens Roesner
Approved by	<i>Dominik Angerer, Lydia Kothmeier, Marisa Pereira</i>

# 1. Purpose of this Whistleblowing Policy

This policy is designed based on the rules set in the EU Whistleblower Directive<sup>1</sup> and the Austrian Whistleblower Protection Act<sup>2</sup> implementing the EU Directive in the jurisdiction where Storyblok is located. With this policy Storyblok (Storyblok GmbH and its affiliates, hereinafter “Storyblok” or “we”, “us”, “our”) aims to maintain the highest standards of integrity, transparency, and ethical conduct in all aspects of its business operations. Storyblok is committed to give different parties a way to speak up and we want to provide employees, contractors, suppliers, customers, partners and other stakeholders (hereinafter the “whistleblower” or “you”) with a mechanism to report any concerns or suspicions about illegal activities, unethical behaviour, or other illegal actions within the company.

Additionally, safeguarding our values and code of conduct are cornerstone to our business success. All Storyblok team members are expected to enhance and uphold acceptable levels of conduct, attendance, and job performance.

## 2. Scope

### Who can report breaches?

Breaches mentioned here can be reported by any Storyblok team member, supplier, partner, customer, investors or any third party that has information about an illegal action as stated herein.

---

<sup>1</sup> [DIRECTIVE \(EU\) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2019 on the protection of persons who report breaches of Union law](#)

<sup>2</sup> [Austrian HinweisgeberInnenschutzgesetz, HschG](#)

## Which infringements can be reported?

The infringement reporting or whistleblowing policy applies to concerns about suspected or actual criminal conduct, unethical conduct, g **illegal actions and any breach of law** in one of the following areas:

- (i) public procurement;
- (ii) financial services, products and markets, and prevention of money laundering and terrorist financing;
- (iii) product safety and compliance;
- (iv) transport safety;
- (v) protection of the environment;
- (vi) radiation protection and nuclear safety;
- (vii) food and feed safety, animal health and welfare;
- (viii) public health;
- (ix) consumer protection;
- (x) protection of privacy and personal data, and security of network and information systems;
- (xi) prevention and punishment of criminal offenses pursuant to Sections 302 to 309 of the Austrian Criminal Code (Strafgesetzbuch, StGB; this includes for example, abuse of authority, bribery and corruptibility).

Furthermore, also breaches affecting the financial interests of the Union and breaches relating to the internal market, including breaches of competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

## What are the requirements to a report?

Following cumulative requirements need to be met to qualify a whistleblower report to be protected under applicable law:

- (i) the whistleblower has information that he/she can claim to be correct according to general experience;
- (ii) the information describes a fact or situation which suggests the suspicion of a violation of the abovementioned law according to general experience (with average general knowledge, which does not necessarily include legal knowledge);
- (iii) the whistleblower is subjectively convinced of the correctness of the information and that the situation/facts happened;
- (iv) the whistleblower can assume (with the knowledge of a person not familiar with the law, but who has familiarized him/herself with the main features of the applicable law), that he/she is covered by the law and that the suspected violation falls within the legal areas mentioned.

This means that whistleblowers are also protected if the information subsequently proves to be false, but they had reasonable grounds to believe that the information was true.

Whistleblowers do not benefit from protection if they intentionally or grossly negligently disseminate false information (e.g. spam or obviously not based on true facts). Furthermore, Storyblok reserves the right to claim for damages and administrative penalties apply in case of intentional misuse.

## 3. Reporting Procedure

### How can reports be made internally to Storyblok?

We encourage everyone to inform us immediately of any infringements. For reporting any infringement Storyblok has created a committee which includes people from different departments and levels. Depending on the report type, people might differ. These people are involved in Storyblok's reporting procedure:

- Lydia Kothmeier, VP of Operations: +43 660 31 45 741 lk@storyblok.com
- Marisa Pereira, VP of People & Organization: marisa.pereira@storyblok.com
- Cristina San Martin, Senior Treasury Analyst: cristina.sanmartin@storyblok.com
- Clemens Roesner, Legal Associate: clemens.roesner@storyblok.com

Any individual who becomes aware of a violation as specified in this policy, should promptly report their concerns. The report can be done verbally or written. They can choose to report through the following channels:

- Dedicated reporting email address [infringement@storyblok.com](mailto:infringement@storyblok.com) (the designated committee will have access to the sent E-Mails)
- If any of the 4 people in the compliance committee are deemed not be neutral enough about the topic or are too close to the person being reported or are the ones about whom a report is being done, the person that wants to report the infringement can address the other people in this committee directly using their email address.
- If you want to report orally you can call the following number +43 660 31 45 741 (VP of Operations)
- Send a google invite for a meeting to [infringement@storyblok.com](mailto:infringement@storyblok.com)

Storyblok encourages everyone to provide their contact details and detailed information when reporting concerns to facilitate effective communication and investigation. Anonymous reporting is also acceptable, and appropriate measures will be taken to protect the anonymity of the reporter. In case you report anonymously (e.g. chose an anonymous email address to send a report to us) we still encourage you to provide a contact option, as in many cases more detailed information is necessary to conduct investigations and you could then answer follow-up questions that may have come up.

The following channels can be used for anonymous reporting:

- Dedicated reporting email address [infringement@storyblok.com](mailto:infringement@storyblok.com) (the compliance committee will have access to the sent E-Mails.)

## Can reports be made externally to someone else?

We encourage everyone to use our internal reporting mechanisms as a fast and direct way to let us know of any infringements. Reports may also be addressed to external reporting channels operated by Austrian government authorities. Reports may be provided to an external authority if it is not possible, not appropriate or not reasonable to handle information in the internal whistleblower system or if internal reporting is unsuccessful or futile. For example, if whistleblowers have reasonable grounds to believe that internal reporting mechanisms have not adequately addressed their concerns, they may report directly to the competent national authorities.

The competent authority is:

- [Federal Bureau of Anti-Corruption and Prevention of Corruption](#) (Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung)  
Reports can be made [here](#).

Please note that other official reporting channels exist for specific infringement claims<sup>3</sup>, including the following channels:

- [Federal Competition Authority](#) (Bundeswettbewerbsbehörde)
- [Financial Reporting Authority](#) (Bilanzbuchhaltungsbehörde)
- [Financial Market Authority](#) (Finanzmarktaufsichtsbehörde)
- [Money Laundering Reporting Office](#) (Geldwäschemeldestelle)

## How are whistleblowers protected?

Storyblok will ensure that there is no retaliation against the person reporting an eligible breach/infringement. We will protect the identity of the whistleblower/ reporting an eligible infringement, and as required by law. The channels for receiving the reports are designed and operated in a secured manner.

Following protection applies:

According to the directive Storyblok will follow the protections for any reporter:

- **Protection of identity:** no disclosure of the identity, unless required by law or the person gives consent
- **Protection against retaliation:** e.g. suspension, lay-off, dismissal, demotion or withholding a promotion, transfer of duties, wage reduction, change in working hours, withholding of training, negative performance assessment or employment reference, no disciplinary measure or financial penalties, harassment, intimidation, discrimination, unfair treatment, early contract termination, failure to renew the contract, etc.

---

<sup>3</sup> Please see Section 15 para. 2 of the Austrian Whistleblower Act (HSchG)

## 4. Handling and investigation

Upon receiving a report, Storyblok will ensure that all concerns are treated seriously, objectively, and in a timely manner. Storyblok will acknowledge the receipt within 7 days. The committee will investigate the topic. The committee will contact you, by your preferred method of communication, to discuss the investigation process and any other matters that are relevant to the investigation.

Storyblok will conduct the investigation based on the information provided, and may ask for additional information. Depending on the topic, the committee will recommend actions. Every report will be handled at least by two people who are part of the committee.

We will take each and every report seriously and do a diligent investigation. This might include interviewing/talking to the person reporting the breach, to the accused party and to other peers or stakeholders that might have observed or witnessed the breach.

The investigation of the topic is done and feedback will be provided by the Committee. Depending on the outcome of the investigation, such feedback may be accompanied by actions (such as warning, immediate termination of the contract, etc.). The committee will provide feedback to the reporter by not exceeding three months from the acknowledgment of the receipt.

## 5. Records and Retention

### Records and Confidentiality

Storyblok will maintain accurate records of all reported concerns, investigations, and outcomes in a confidential manner. Records will be retained for the required period as specified by applicable laws and regulations. We take care to protect the identity of reporters and the confidentiality of personal data. In any case, all record keeping of the reports will be done in compliance with applicable law. The identity of whistleblowers, including information from which the identity can be derived, may be disclosed if an administrative authority, a court or the public prosecutor's office considers this to be essential and proportionate in the context of administrative or judicial proceedings or investigative proceedings under the law. Any risk to the person of the whistleblower will also be taken into account with regard to the validity and seriousness of the allegations made.

### Privacy & Processing of Personal Data

All personal data received or collected will also be processed in accordance with applicable data protection law. We will limit the data processed to fulfill the requirements of applicable law. This includes personal data of the

- name of whistleblowers,
- persons affected by the whistleblowing,
- natural persons who assist whistleblowers in providing information,

- natural persons in the vicinity of the whistleblower who, without supporting the whistleblowing, could be affected by adverse consequences of the whistleblowing, such as retaliatory measures, and
- persons affected by or involved in follow-up measures.

We are authorized to process such data based on Art. 6 para. 1 lit c GDPR (legal obligation) due to the authorization in the applicable law (Art 8 HSchG) . If personal data is processed in the case of information outside the scope of the HSchG, such data is processed on the basis of Art. 6 para. 1 lit f GDPR (legitimate interest). Please see our Privacy Policies on further details how we use and process personal data:

- [Storyblok Privacy Policy](#)
- [Applicant Privacy Policy](#)
- [Storyblok Teammember Privacy Notice](#)

Please note that your personal data (insofar as it can be ascertained or has been disclosed) may be disclosed in certain cases regulated by law. In particular, the provisions of the Austrian Code of Criminal Procedure (StPO) apply if there is an initial criminal suspicion.

## 6. Miscellaneous

### Training and communication

Storyblok will provide internal training on this policy as part of the induction process for all new team members.

### Changes in the Policy

Storyblok may update or change this policy at its sole discretion, at any time, provided that such updates are in compliance with the Whistleblower directive or its implementing laws.

Should any of the actions/processes provided in this policy conflict the provisions of the Whistleblower Directive, the provisions set in the directive shall take precedence.