1. Purpose of Whistleblowing Policy

This policy is designed based on the rules set in the EU Whistleblower Directive\(^1\) and 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 with a mechanism to report any concerns or suspicions about illegal activities, unethical behaviour, or other illegal actions within the company.

Storyblok is committed to give different parties a way to speak up and we want to provide employees, contractors, suppliers, and other stakeholders with a mechanism to report any concerns or suspicions about illegal activities, unethical behaviour, or other wrongdoing 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

The infringement reporting or whistleblowing policy applies to all employees, contractors, suppliers, customers, partners, and other stakeholders of Storyblok. It applies to concerns about suspected or actual criminal conduct, unethical conduct including but not limited to the following illegal actions and any breach of the EU 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;

\(^{1}\) 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
(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;

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.

### 3. Reporting Procedure

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.rosner@storyblok.com

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

- Dedicated reporting email address 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

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.

The following channels can be used for anonymous reporting:

- Dedicated reporting email address infringement@storyblok.com (the compliance committee will have access to the sent EMail.)
Who can report breaches?

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

Prohibition of retaliation

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

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

- No disclosure of the identity, unless the person gives consent
- Protection against 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.

4. Handling and investigation

Upon receiving a report, Storyblok will ensure that all concerns are treated seriously, objectively, and in a timely manner within 5 business 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.

Where you have chosen to remain anonymous, your identity will not be disclosed to any other person outside of the designated committee. 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.

---

If there are any discrepancies between the Whistleblower directive and this section, the procedure set in the Whistleblowing directive for matters mentioned in section 1 (i) will take precedence over the procedure detailed in this section.
5. Records and Retention

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 resulting from Section 1 (i) will be done in compliance with Article 18 of the Whistleblower directive.

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.

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.