

The national and European courts have recently been able to clarify several legal issues, providing a reason to review and adjust existing compliance and IT security management systems, in-house policies and employee training programs in order to avoid infringements and the associated financial loss and damage to a company's public image.

The following presents a selection of the issues that can arise time and again when a company is using new media, for example, within the context of an informative company homepage, an interactive social media presence or an online shop, and which should be taken into consideration when revising in-house IT policies.

Exclusion of Liability Through Disclaimers

It is a common misconception that a disclaimer is sufficient for denying responsibility for the content on a homepage. It is, however, not possible to exclude liability in such a blanket statement because it is always dependent on whether a company's own or third-party content is being made available. If content originating from third parties is, for example, integrated into a homepage after verifying and editing the content, liability for default and damages still exists for any legal violations, as in the case of a company's own infringing content.

There may be a duty to immediately delete or even omit telecommunications media, which is clearly recognizable as third-party content, if notice is given of the infringing content but a response does not occur in a timely manner, and similar infringements are not prevented in the future.

Conclusion: It is not the wording of the disclaimer, but the actual manner of integrating the content into a homepage that is decisive for any potential liability.

Infringements of Intellectual Property Rights

Anyone who includes protected third-party content (e.g., text, photos, films, trademarks, designs) on a homepage is obligated to check whether the use of the content is permitted or requires the consent of the legal owner, e.g., by way of a license. In the case of works protected by copyright, it must also be considered that a right to be identified as the author generally exists and, even in the case of content subject to Creative Commons licenses, only limited use is often permitted.

Conclusion: Any uncertainty in terms of the right to use protected content is always determined at the expense of the user. However, even those who purchase licenses from professional agencies should obtain a contractual guarantee that the rights are acquired free from any opposing rights of third parties and include a duty to indemnify against the claims of third parties.

Unauthorized Reproduction Through Hyperlinks/Frames

Hyperlinks are the central means for referencing data, which can be used to link available information on the Internet. If reference is made to the content of third parties using a link on a company's homepage, the content can then also appear in a frame upon being accessed (inline link), i.e., surrounded by the homepage containing the link, so that the user is given the impression that the content originates from or is embedded in the homepage, which is visible as a frame. It has now been clarified that the use of hyperlinks and framing is a form of public reproduction that does not require the consent of the copyright owner if the owner has made the content freely accessible on the Internet without any technical restrictions (ECJ, Decision of 21 October 2014 – C-348-13; ECJ, Decision of 13 February 2014 – C-466/12).

If freely accessible content of third parties is directly linked, there are no problems in this respect. However, the situation becomes critical if content from intermediary (video) portals is linked via hyperlinks/frames but the copyright owner has not agreed to allow free access to such content or limits the access at a later date, for example, to paying subscribers, while this restriction is not implemented on the intermediary portal. The content is then being addressed to a new – non-paying – audience via the hyperlink/frame, which constitutes an unauthorized public reproduction of the content.

Conclusion: It is therefore advisable to check all of the hyperlinks on the homepage of one's own company and to only include links to content which directly originates from the copyright owner or a reliable license holder.

Infringements of Personality Rights on Blogs and Rating Portals

Guest books, blogs, feedback and rating functions on the Internet can provide companies with valuable information about the impression their products, services and campaigns leave with their end customers.

The advantages of the option to use these functions anonymously are accompanied by an increased risk of misuse leading to infringements of personality rights, e.g., through false representation and defamation. This can thereby concern not only individual natural persons, but also companies whose products and services are the subject of false and defamatory statements, because the economic and social reputation of companies is also protected by law.

Conclusion: Any feedback and ratings on the Internet should therefore be screened and filtered as part of careful reputation management in order to prevent damages to an individual's or company's image at an early stage and be able to assess the necessity of legal action in proper time.

Liability and Duties of Blog and Rating Portal Operators for Infringements of Personality Rights

The operator (hosting services provider) of a blog or rating portal needs to develop a systematic complaint management concept and use filtering software in order to be able to take the appropriate actions quickly if concerned individuals complain of infringements of personality rights in blog entries or reviews of anonymous users. The hosting provider could otherwise be liable as the disrupter for cease-and-desist claims resulting from the statements made by third parties (German Federal Court of Justice, Default Judgment of 25 October 2011 – VI ZR 93/10).

Conclusion: In this connection, providing conscientious legal training for the responsible employees of the hosting provider and the preparation and implementation of clear complaint management guidelines is imperative in order to avoid any liability for the statements of third parties. It must also thereby be kept in mind that if, for example, the host provider discloses the personal data of a user, who has made an anonymous statement, to a private person, whose personality rights have been violated, this breaches data protection law (German Federal Court of Justice, Judgment of 1 July 2014 - VI ZR 345/13). The disclosure of the personal data to an investigating public prosecutor, however, is permitted and can prevent measures such as searches by the authorities.

If you would like further information about these issues or assistance in creating or revising in-house IT policies, please contact your Squire Patton Boggs lawyer or one of the individuals listed in this publication.



Dr. Annette Demmel

Partner

Rechtsanwältin, Certified Specialist for Information Technology Law (*Fachanwältin für Informationstechnologierecht*)

T +49 30 726 16 8108

E annette.demmel@squirepb.com

Squire Patton Boggs (US) LLP

Unter den Linden 14

10117 Berlin



Maxim Eifinger

Associate

Rechtsanwalt, Certified Specialist for Information Technology Law (*Fachanwalt für Informationstechnologierecht*)

T +49 69 1739 24 38

E maxim.eifinger@squirepb.com

Squire Patton Boggs (US) LLP

Taunusanlage 17

60325 Frankfurt am Main

The contents of this update are not intended to serve as legal advice related to individual situations or as legal opinions concerning such situations nor should they be considered a substitute for taking legal advice.

© Squire Patton Boggs.