Transnational Aspects of Compliance

CEJ
COMPLIANCE ELLIANCE JOURNAL

Content Curators:
Michele DeStefano (University of Miami School of Law)
Dr. Hendrik Schneider (University of Leipzig Faculty of Law)

ISSN 2365-3353
Volume 6 • Number 2
Fall 2020

Compliance Elliance Journal (CEJ)
Volume 6, Number 2, 2020
ISSN: 2365-3353
This version appears in print and online. CEJ is published twice per year, in spring and fall.

Title: Transnational Aspects of Compliance

Content Curators:
Michele DeStefano, University of Miami School of Law and LawWithoutWalls
Prof. Dr. Hendrik Schneider, Attorney at law

Technical Support:
Luisa Wermter

Website: www.cej-online.com

Email: info@cej-online.com

Address:
Taunusstrasse 7
65183 Wiesbaden, Germany

Telephone: +49 611 531 658 41

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

Transnational Aspects of Compliance

TABLE OF CONTENTS

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

EDITORIAL

TRANSNATIONAL ASPECTS OF COMPLIANCE

In view of the presidential election in the USA, the extensive worldwide reporting once again made it clear how significant the global impact of events within the USA is and how much attention they attract. In this issue we focus on the transfer of problems and ideas from the USA in connection with compliance, in particular from a European perspective (German-speaking countries).

Apart from social phenomena such as the MeToo debate or the Black Lives Matter movement, which have an impact not only on the private sphere but also on the culture within companies, sanction lists for companies and the compliance risks of Block Chain Technology are also highlighted in the contributions of our renowned authors.

Finally, the series on the different national approaches to the criminal liability of associations with a view to Austrian law is continued.

With our best regards,

Michele DeStefano & Hendrik Schneider
Founder and Content Curators of CEJ

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

COMPLIANCE IN TIMES OF DISCRIMINATION[1]

Rita Pikó & Laurenz Uhl

AUTHOR

Dr. Rita Pikó, LL.M. (Exeter), is an attorney at law in Zurich in her law firm Pikó Uhl Rechtsanwälte AG, admitted in Switzerland and Germany and specialized in corporate compliance and internal investigations. Dr. Pikó is a regular speaker at the qualification program for supervisory board members (Exzellenzprogramm für Aufsichtsräte) at the Frankfurt School of Management & Finance. She lectures in compliance at the Zurich University of Applied Sciences (ZHAW), the University of Liechtenstein as well as the Burgenland University of Applied Sciences.

Dr. Laurenz Uhl, LL.M. (Exeter), is an attorney at law in Zurich in his law firm Pikó Uhl Rechtsanwälte AG, admitted in Switzerland and Germany and specialized in corporate compliance and internal investigations.

ABSTRACT

Coming to terms with discrimination in the workspace (including sexual harassment and racism) as an integral part of compliance in Germany and Switzerland in recent years, profit-oriented companies and non-profit organizations have increasingly had to deal with discrimination, especially sexual assault and racist behavior. This article deals with how these risks can be addressed in compliance management systems, which preventive measures are recommended and which special features should be taken into account when investigating and dealing with such incidents internally.

[1] This article was first published in German in the BetriebsBerater 21/2020, p. 1205-1214. The Authors are very grateful to the BetriebsBerater allowing them to publish this translation including an update.

TABLE OF CONTENTS

I. INTRODUCTION

A modern Compliance Management System (CMS) not only covers the prevention and combating of white-collar crime, but also cases of discrimination and in particular sexual harassment and racist behavior in the workspace.[2] The reasons for this lie primarily in economic factors, legal requirements and a value-based understanding of compliance. The combination of these three aspects makes it clear what position discrimination incidents in the workspace (including sexual harassment and racism) should have within CMS today.

The growing number of studies on sexual harassment in the workspace highlights the often unnoticed dimension of the problem. In the German-speaking countries, for example, about half of the population made their first-hand experience of sexual assault: in Switzerland, about 55% of female employees and 49% of male employees have been confronted with sexual harassment during the course of their working lives.[3] According to a study by the German Federal Anti-Discrimination Office, about half of the people questioned have experienced legally prohibited harassment at work.[4] And in Austria, approximately 56% of employed women have been sexually harassed at their workplace.[5] Even lawyers are not safe from discrimination and sexual harassment at their workplaces, as the study published in 2019 by the International Bar Association shows: one of 3 woman and one of 14 men surveyed were sexually harassed at work.[6]

Robust studies on racial discrimination specifically in the workspace are currently scarce or non-existent for Switzerland, Germany or Austria. This may change with the increased significance of this topic, fostered in particular by the "Black Lives Matter" movement. Reports on racial discrimination in Swit-zerland show that the workspace is the area in which – consistently over years – discriminatory behavior was most frequently reported.[7] Pursuant to a study from 2019 in Germany, 21% of the

[2] All internet sources based on the original article were last accessed on 4/15/2020; this article deals with *unwanted* sexual assaults, harassment, racial and other discrimination. With regard to consensual relations in the workspace and their regulation in a code of conduct, see the Wal-Mart decision of the LAG Düsseldorf, 11/14/2005 – 10 TaBV 46/05, BB 2006, 335 Ls, NZA-RR 2006, 81.

[3] Risiko und Verbreitung sexueller Belästigung am Arbeitsplatz, Eine repräsentative Erhebung in der Deutschschweiz und in der Romandie, 2008. According to a recent nationwide survey of women aged 16 and over, 73% consider sexual harassment to be very common, 64% personally know women who have been sexually harassed, with 33% of sexual harassment occurring in the workspace, *Jans u. a.,* gfs. Bern, May 2019, 7, 9 u. 12.

[4] Studie der Antidiskriminierungsstelle des Bundes, Sexuelle Belästigung am Arbeitsplatz dated 3/3/2015, see https://www.antidiskriminierungsstelle.de/SharedDocs/Downloads/DE/publikationen/Umfragen/Handout_Umfrage_sex_Belaestigung_am_ArbPlatz_Beschaeftigte.pdf;jsessionid=31664677A3430789E110157E2DEC7EE5.2_cid340?__blob=publicationFile&v=4.

[5] This is also confirmed by the Working Climate Index (Arbeitsklima Index) November 2018, according to which 56% of employed women in Austria have been sexually harassed in their workspace; Kammer für Arbeiter und Angestellte für Oberösterreich, see https://ooe.arbeiterkammer.at/beratung/arbeitundgesundheit/arbeitsklima/arbeitsklima_index/Arbeitsklima_Index_2018_November.html.

[6] *Kieran Pender*, Us Too?, Bullying and Sexual Harassment in the Legal Profession, International Bar Association, May 2019, 8 („2019 IBA Study"), see https://www.ibanet.org/bullying-and-sexual-harassment.aspx. In this study, 6 980 interviews with lawyers in law firms, companies, bar associations, courts and public services were conducted in 135 countries.

[7] For Switzerland see „Rassistische Diskriminierung in der Schweiz. Bericht der Fachstelle für Rassismussbekämpfung 2018" issued by Fachstelle für Rassimusbekämpfung FRB, see https://www.edi.admin.ch/dam/edi/de/dokumente/FRB/Neue%20Website%20FRB/Monitoring%20und%20Berichterstattung/Bericht/FRB%20Bericht%202018.pdf.download.pdf/Rassistische-Diskriminierung%202018_de_WEB.pdf.

questioned employees reported having been victim or witness of racial discrimination in the workspace.[8] Often, such discrimination goes hand in hand with other forms of discrimination such as bullying or mobbing.[9] It is to expected that the number of unreported cases of racist discrimination in the workspace is high. [10]

II. ECONOMIC FACTORS

A. Changes in the Social Perception and Assessment of Discrimination Cases

Harvey Weinstein, formerly one of Hollywood's most influential producers, was sentenced to 23 years in prison by the Supreme Court of New York on March 11, 2020. Two weeks earlier, he was found guilty by a jury court of having committed a criminal sex act and rape in the third degree of women from his professional environment. Weinstein is registered in a publicly accessible register for sexual criminals.[11] The Weinstein case follows on from other sexual assaults by well-known personalities in the industrial sector, such as that of US actor Bill Cosby and Bill O'Reilly, television journalist at US channel Fox News, and Roger Alies, former CEO of Fox News. The testimonies of the victims of Weinstein and Co. made the hashtag #MeToo known worldwide as a campaign against all forms of sexual assault.[12]

#MeToo's main effect has been to ensure that victims of sexual assault are taken seriously, can hope to be heard and have their evidence carefully considered, even if there is no actual proof, only circumstantial evidence.[13]

[8] Diversity & Inclusion Study 2019 by Glasdoor, see https://about-content.glassdoor.com//app/uploads/sites/2/2019/10/Glassdoor-Diversity-Survey-Supplement-1.pdf. For Austria, no comparable studies could be identified. The Austrian ZARA (Zivilcourage und Anti-Rassismus Arbeit) noted in its "Rassimus Report 2019" a number of 59 cases in or in connection with the workspace.

[9] Rassistische Diskriminierung in der Schweiz. Bericht der Fachstelle für Rassismussbekämpfung 2018" issued by Fachstelle für Rassimusbekämpfung FRB, see https://www.edi.admin.ch/dam/edi/de/dokumente/FRB/Neue%20Website%20FRB/Monitoring%20und%20Berichterstattung/Bericht/FRB%20Bericht%202018.pdf.download.pdf/Rassistische-Diskriminierung%202018_de_WEB.pdf.

[10] See Rassistische Diskriminierung in der Schweiz. Bericht der Fachstelle für Rassismussbekämpfung 2018" issued by Fachstelle für Rassimusbekämpfung FRB, see https://www.edi.admin.ch/dam/edi/de/dokumente/FRB/Neue%20Website%20FRB/Monitoring%20und%20Berichterstattung/Bericht/FRB%20Bericht%202018.pdf.download.pdf/Rassistische-Diskriminierung%202018_de_WEB.pdf, p. 48.

[11] *Langer*, Historisches Urteil für #MeToo-Bewegung, NZZ dated 3/12/2020, see https://www.nzz.ch/panorama/urteil-gegen-harvey-weinstein-ld.1545842. Harvey Weinstein is facing further proceedings, NZZ dated 4/10/2020, see https://www.nzz.ch/panorama/harvey-weinstein-zu-23-jahren-gefaengnis-verurteilt-ld.1532074.

[12] *Tenz/Fischer*, Der „Fall Weinstein" – Chronik eines Skandals, DW dated 3/9/2020, see https://www.dw.com/de/der-fall-weinstein-chronik-eines-skandals/a-51881759.

[13] *Binswanger/Widmer*, Im Zweifel für die Opfer, Tagesanzeiger dated 2/25/2020, see https://www.tagesanzeiger.ch/kultur/im-zweifel-fuer-die-perspektive-der-opfer/story/12636044.

This is not an exclusive problem of the US film and television industry. Incidents of sexual discrimination occur regardless of industry or country: They can, inter alia, be found in the financial[14] and consulting[15] industry, at universities[16], opera houses[17] or royal houses[18], at NPOs[19] and in politics[20].

The typical pattern in many of these cases is the exploitation of hierarchical or economic positions of power. It is also typical that cases of discrimination and sexual harassment in the workspace are in most cases not made public at all.[21] The reasons for this are mainly the dread of the consequences (financial or professional ruin, loss of reputation), the status of the discriminating person, the normalization of such incidents in the workspace, difficulties in providing evidence and the fear of having to report and relive what has been experienced over and over again.[22] In the #MeToo movement, those affected have found a community that allows them to step out of the role of victim and to defend themselves. This is accompanied by the disappearance of the previous tacit tolerance of the exploitation of power positions for sexual discrimination and the trivialization of such behavior.

Ubisoft, a prominent French creator and publisher of video and online games with over 16,000 employees worldwide, was accused in Summer 2020 of tolerating a culture of sexual harassment and

[14] Credit Suisse: Interne Untersuchung nach Firmenausflug, Finews.ch dated 6/27/2018, see https://www.finews.ch/news/banken/32335-cs-investmentbanker-untersuchung-usa-praktikantin-belaestigung; Sexual Harasment: Credit Suisse feuert zwei Londoner Banker, Finews.ch dated 8/23/2018, see https://www.finews.ch/news/banken/32970-credit-suisse-sexuelle-belaestigung-entlassung. Big accounting firms are affected too: https://www.tagesanzeiger.ch/wirtschaft/standardey-stellt-mitarbeiter-nach-vorwuerfen-per-sofort-frei/story/22803713.

[15] *Binswanger*, „Zeig doch deine Assets ;-)", Tagesanzeiger dated 12/11/2018, see https://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/zeig-doch-deine-assets/story/23578823.

[16] *Rau*, Sie wirft Professor Übergriffe vor – und fühlt sich nun abgekanzelt, Tagesanzeiger dated 12/18/2019, see https://www.tagesanzeiger.ch/schweiz/standard/was-darf-eine-betroffene-nach-einem-missbrauchsfall-erwarten/story/30203736; *Pfändler*, Nach Vorwurf der sexuellen Belästigung: ETH-Professor gibt Rücktritt bekannt, NZZ dated 1/29/2019, see https://www.nzz.ch/zuerich/nach-vorwurf-der-sexuellen-belaestigung-eth-professor-gibt-ruecktritt-bekannt-ld.1455635?reduced=true; *Petersen*, Einzelfälle? Strukturwandel? Zivilcourage?, Hochparterre dated 2/20/2019, see https://www.hochparterre.ch/nachrichten/architektur/blog/post/detail/einzelfaelle-strukturwandel-zivilcourage/1550606879/.

[17] *Widmer*, #MeToo: Placido Domingo ist der nächste Täter, Tagesanzeiger dated 2/25/2020, see https://www.tagesanzeiger.ch/kultur/klassik/metoo-placido-domingo-ist-der-naechste-taeter/story/14340543.

[18] US-Behörden wollen Prinz Andrew zum Fall Jeffrey Epstein befragen, Zeit Online dated 1/27/2020, see https://www.zeit.de/gesellschaft/zeitgeschehen/2020-01/sexueller-missbrauch-jeffrey-epstein-prince-andrew-fbi.

[19] *Pikó*, CB 2018, 221, 222.

[20] On the resignation of the British Secretary of State for Defense Michael Fallon, Süddeutsche dated 11/1/2017, see https://www.sueddeutsche.de/politik/grossbritannien-verteidigungsminister-fallon-tritt-zurueck-1.3732225?print=true; Vice-President of Israel resigns due to allegations of misconduct, DW dated 12/20/2015 see https://www.dw.com/de/israels-vizepremier-tritt-wegen-missbrauchsvorwürfen-zurück/a-18931246; Unia gibt Roman Burger den Schuh, Handelszeitung dated 9/16/2016, see https://www.handelszeitung.ch/politik/unia-gibt-roman-burger-den-schuh-1204108; Resignation of the St. Galler canton council member Marcel Dietsche, Tagblatt dated 5/1/2019, see https://www.tagblatt.ch/schweiz/verdacht-auf-sexuelle-belaestigung-kantonsrat-marcel-dietsche-tritt-zurueck-ld.1115212.

[21] According to the 2019 IBA study, 57% of mobbing incidents and 75% of sexual harassment incidents go unreported.

[22] *Pender*, Us Too?, Bullying and Sexual Harassment in the Legal Profession, International Bar Association, May 2019, p. 8, see https://www.ibanet.org/bullying-and-sexual-harassment.aspx.; *Miller*, Know My Name, New York 2019; *Farrow*, Catch and Kill, Lies, Spies and a conspiracy to protect predators, 2019.

racist behavior by its managers. As a consequence, at least six managers had to leave the company.[23] Zalando was confronted with the accusation - published via social media - of racist behavior by some of its employees. Zalando reacted in August 2020 by conducting an internal investigation and publishing a clear statement that such behavior shall not be tolerated.[24] These recently published cases indicate that racist discrimination in the workspace is getting more public attention and that organizations will have to deal with such cases more actively.

B. Costs of Damage to Reputation

Accusations of sexual harassment, racism or other discrimination in the workspace can pose a serious risk - for companies and the accused themselves - due to the damage it may cause to their reputation.

The economic consequences of the loss of reputation can be rapid and dramatic, as the following examples show: On October 5, 2017, *Jodi Kantor* and *Megan Twohey* published an article in the New York Times accursing *Harvey Weinstein* of sexual harassment.[25] Three days later *Harvey Weinstein* was fired by his own company, The Weinstein Company, and nine days later *Harvey Weinstein* resigned from the company's management. The company filed for bankruptcy just under five months later on March 19, 2018.[26] Former Uber employee *Susan Fowler* published a blog on 2/10/2017 about the sexist culture at Uber and the ignoring by Uber of the relevant internal reports. The following day an internal investigation was launched and later published as the Holden Report.[27] 215 discrimination cases were investigated and 20 Uber employees were dismissed. The Managing Director of Uber in Asia, *David Bonderman*, member of the Executive Board, and the co-founder, majority shareholder and CEO *Travis Kalanick* also had to leave Uber in the wake of the scandal.[28] Television journalist *Gretchen Carlson* sued the then CEO of Fox News, *Roger Ailes*, for sexual harassment.[29] Subsequently, not only *Roger Ailes* but also television journalist *Bill O'Reilly* had to leave the company without notice. *Carlson* received a payment of USD 20 million as compensation for the injustice suffered. As a result, more than 60 major companies cancelled their TV commercials at Fox News. In the end, 21st Century Fox Inc. also paid a settlement sum of USD 90 million to shareholders who had sued management for lack of supervision in connection with the sexual harassment scandals on its Fox News Channel.[30]

[23] *Schreier*, Ubisoft Family Accused of Mishandling Sexual Misconduct Claims, see https://www.bloomberg.com/news/articles/2020-07-21/ubisoft-sexual-misconduct-scandal-harassment-sexism-and-abuse.

[24] https://corporate.zalando.com/de/newsroom/news-storys/zalando-veroeffentlicht-untersuchungsergebnisse-und-verstaerkt-massnahmen-fuer.

[25] *Kantor/Twohey*, Harvey Weinstein Paid Off Sexual Harassment Accusers for Decades, The New York Times dated 10/15/2017, see https://www.nytimes.com/2017/10/05/us/harvey-weinstein-harassment-allegations.html.

[26] *Tenz/Fischer*, Der „Fall Weinstein" – Chronik eines Skandals, DW dated 3/9/2020, see https://www.dw.com/de/der-fall-weinstein-chronik-eines-skandals/a-51881759.

[27] Uber Report: Eric Holder´s Recommendations for Change, The New York Times dated 6/13/2017, see https://www.nytimes.com/2017/06/13/technology/uber-report-eric-holders-recommendations-for-change.html.

[28] *Isaac*, Uber Founder Travis Kalanick Resigns as C.E.O., The New York Times dated 6/21/2017, see https://www.nytimes.com/2017/06/21/technology/uber-ceo-travis-kalanick.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news.

[29] *Remke*, Eine Afroamerikanerin nannte er sein „heißes Stück Schokolade", Welt dated 4/20/2017, see https://www.welt.de/vermischtes/article163873247/Eine-Afroamerikanerin-nannte-er-sein-heisses-Stueck-Schokolade.html.

[30] Reuters dated 11/21/2017, see https://www.reuters.com/article/us-fox-settlement/21st-century-fox-in-90-million-settlement-tied-to-sexual-harassment-scandal-idUSKBN1DK2NI.

Acute discrimination cases are not the only threat to companies: Inadequately handled cases can also generate unwelcome publicity, as the case of an auditing firm shows.[31] The cases of discrimination by Oxfam employees in Haiti occurred in 2011 but were picked up again by the UK media in early 2018, resulting in the loss of 7,000 donors within ten days and ultimately a GBP 16 million loss of funds.[32]

C. Other Negative Consequences

According to the study by *Does/Gundemir/Shih*[33], even a single accusation of sexual harassment may dramatically worsen the public perception of an entire organization. Not only is the organization seen as less fair and just than an organization without such an accusation. This organization is also seen as less fair and just compared to organizations against which allegations of financial misconduct (e.g. fraud) are made. According to the study, accusations of sexual harassment are more likely to be seen as an indication of a problem with the company's culture rather than a misbehaving employee in the sense of a "rotten apple". The study states that the interviewees also draw negative conclusions from these accusations regarding fairness with regard to hiring and promotion in the company concerned. The loss of reputation may have a correspondingly negative effect on the hiring of new talent and the review of employees.[34]

The topic is recently also being included in the legal documentation of M&A deals: M&A contracts are increasingly beginning to include assurances in the form of so-called "Weinstein clauses" ("#MeToo Rep") in order to limit possible negative effects.[35] Sources of damage can be legal proceedings, loss of reputation as well as indirect cost sources, such as loss of employees and recruiting difficulties due to negative "employer branding", reduced performance or a worsened working atmosphere.[36] According to a study, 45 of approximately 1,200 M&A transactions filed with the SEC in 2018 contained such assurances.[37] It is likely that German or Swiss companies with references to the US capital market will also have to deal with such assurances in contracts in the future. Such representations may need to be extended to include racist discrimination, too.

Finally, more and more investors are looking at investments based on ESG criteria (environmental, social and governance). This not only concerns ecological issues, but also questions of justice and honesty. Powerful investors such as Blackrock, State Street and Vanguard expect a more balanced

[31] *Binswanger/Alich*, #MeToo bei EY: Kadermann per sofort freigestellt, Tagesanzeiger dated 12/14/2018, see https://www.tagesanzeiger.ch/wirtschaft/standardey-stellt-mitarbeiter-nach-vorwuerfen-per-sofort-frei/story/22803713.

[32] *O`Neill*, Oxfam to cut staff after Haiti scandal leaves £16m shortfall, The Times dated 1/23/2020, see https://www.thetimes.co.uk/article/oxfam-to-cut-staff-after-haiti-scandal-triggers-16m-shortfall-j763r7fr0.

[33] *Does/Gundemir/Shih*, Research: How Sexual Harassment Affects a Company`s Public Image, Harvard Business Review dated 6/11/2018, see https://hbr.org/2018/06/research-how-sexual-harassment-affects-a-companys-public-image.

[34] For example, PWC studies show that millennials consider the reputation of their employer to be important when choosing a job, PWC, The female millennial, a new area of talent, 2015, see https://www.pwc.com/femalemillennial.

[35] *Balthasar-Wach/Hofbauer*, juridikum 2019, 326 et seq.

[36] *Balthasar-Wach/Hofbauer*, juridikum 2019, 326, 327.

[37] *Peters/Clabaugh*, The Impact of Social, Political and data Privacy Issues on M&A Transactions, Intelligize Special Report, 3/26/2019, 4.

gender distribution in management bodies.[38] From here, it is no longer far from the idea that investors expect companies to treat sexual harassment, racist as well as other discrimination incidents (or the corresponding risks) just as professionally as other compliance incidents.

D. Conclusion

The cases listed are examples of the substantial business risks involved in discrimination cases, in particular, sexual harassment and racist discrimination incidents in the workspace. In many cases, even a public accusation of such behavior is sufficient to cause considerable damage to the company's reputation[39] - not to mention the demoralization and frustration of employees. In times of #MeToo and other social media campaigns, the public dissemination of such accusations is unstoppable. This makes it clear that the damage potential of (sexual) discrimination within the company is approaching other substantial corporate risks.

III. SELECTED LEGAL FACTORS

In connection with discrimination in the workspace, including sexual harassment and racism, employers are subject to certain legal obligations. It would go far beyond the scope of this article to cover all relevant legal provisions. The following explanations are a limited selection of certain legal aspects in the context of discrimination in the workspace.[40]

A. Definition of Discrimination

The starting point for the legal definitions of sexual harassment and racism in the workspace in both Germany and Switzerland is the definition of the general prohibition of discrimination in employment relationships.

1. Discrimination

The definition of discrimination in the workspace in German law is laid down in the General Equal Treatment Act (Allgemeines Gleichbehandlungsgesetz, AGG).[41] According to Section 1 AGG, the purpose of the law is to "prevent or eliminate discrimination on the grounds of race or ethnic origin, gender, religion or belief, disability, age or sexual identity". According to Section 6 AGG, the provisions of the AGG apply to the relationship between employees and employers.[42] Section 1 AGG does not

[38] *Meier*, Verwaltungsrätin dringend gesucht, Tagesanzeiger dated 2/12/2018, see https://www.tagesanzeiger.ch/wirtschaft/standardverwaltungsraetin-dringend-gesucht/story/27061853.

[39] See, for example, the media coverage of the #MeToo case at the Swiss Federal Criminal Court, which turned out not to be a case: *Knellwolf*, Sex – und Mobbingvorwürfe am Bundesstrafgericht, Tagesanzeiger dated 2/1/2020, see https://www.tagesanzeiger.ch/schweiz/standard/das-bundesstreitgericht/story/21337041.

[40] In particular, criminal law, data protection law, public law aspects and employee participation rights are not dealt with here.

[41] Allgemeines Gleichbehandlungsgesetz dated 8/14/2006 (BGBl. I S. 1897), last modified by Article 8 SEPA-Begleitgesetz vom 4/3/2013 (BGBl. I S. 610). The AGG converts the European legal basis, RL 2000/42/EG, RL 2000/78/EG, RL 2004/113/EG and RL 2006/54/EG into national law.

[42] *Bauer/Krieger/Günther*, Allgemeines Gleichbehandlungsgesetz und Entgelttransparenzgesetz, 5. Aufl. 2018, § 6, Rn. 2.

contain any specific facts or legal consequences of its own, so that it only acquires significance in conjunction with other provisions of the AGG.[43]

The legal framework for discrimination in employment relationships in Switzerland is narrower. The Swiss Federal Act on Equal Opportunities for Men and Women (Gleichstellungsgesetz, CH-GlG)[44] aims to promote the actual equality of women and men (Article 1) and thus focuses on gender equality in employment relationships. The CH-GlG thus only regulates discrimination in employment relationships based on gender, but not discrimination based on other characteristics such as racism. Accordingly, the scope of the prohibition of discrimination in Article 3 CH-GlG is narrowly defined: "Employees may not be discriminated, either directly or indirectly, on grounds of their gender, in particular on the grounds of marital status, family situation or, in the case of female employees, pregnancy".

2. Sexual Harassment in the Workspace

Both the AGG and the CH-GlG each contain a specific definition of sexual harassment in the workspace.

According to Section 3 paragraph 4 AGG, sexual harassment is "a disadvantage in relation to Section 2 paragraph 1 no. 1 to 4, if an unwanted, sexually explicit conduct, including unwanted sexual acts and requests for such acts, sexually explicit physical contact, comments of sexual content as well as unwanted showing and visible affixing of pornographic images, has the purpose or effect of violating the dignity of the person concerned, in particular if an environment characterized by intimidation, hostility, humiliation, degradation or insult is created."

The AGG distinguishes between physical, verbal and non-verbal sexual harassment. In this context, even a one-off specific sexual behavior may constitute a criminal offence.[45] This definition is based on the idea of the right to sexual self-determination: Anyone can decide for themselves about an intrusion into the private sphere through physical contact. For example, the BAG has repeatedly regarded the intentional touching of primary or secondary sexual characteristics of another person as sexually determined in the sense of Section 3, paragraph 4 AGG because it is an assault on the intimate physical sphere.[46]

Other acts which do not directly have sexuality as their object, such as hugging, may be qualified as sexual as a result of a sexual intention pursued with them.[47] Whether an act is deemed to be sexual within the meaning of Section 3 paragraph 4 AGG does not depend solely on the subjectively desired goal of the person acting. According to the German Federal Labour Court (Bundesarbeitsgericht, BAG), sexual motivation is also not necessarily required. Rather, such sexual harassment is often an expression of hierarchies and the exercise of power rather than of sexually determined lust.[48]

[43] *Bauer/Krieger/Günther*, Allgemeines Gleichbehandlungsgesetz und Entgelttransparenzgesetz, 5. Aufl. 2018, § 1, Rn. 1.

[44] Bundesgesetz über die Gleichstellung von Frau und Mann dated 3/24/1995, SR 151.1, AS 1996 1498; effective 7/1/2020, AS 2019 2815.

[45] BAG, 6/29/2017 – 2 AZR 302/16, Rn.17.

[46] BAG, 6/29/2017 – 2 AZR 302/16 and BAGE 150, 109.

[47] BAG, 6/29/2017 – 2 AZR 302/16, Rn.18 with references to further BAG judgements.

[48] BAG, 6/29/2017 – 2 AZR 302/16, Rn.19; *Linde*, BB 1994, 2412, 2415.

According to Section 3 paragraph 4 AGG, the decisive factor for the assessment of the conduct is ultimately whether the person concerned objectively recognizably experiences the conduct as undesirable.[49] The prerequisite that the undesired behavior violates or intends to violate the dignity of the person concerned acts as an objective criterion.[50] It protects against hypersensitivity and abuse.

Article 4 CH-GlG is systematically structured in a comparable manner, according to which sexual harassment is expressed as a special case of the general prohibition of gender discrimination in employment relationships regulated in Article 3 CH-GlG. According to Article 4 CH-GlG, sexual discrimination is defined as "any harassing behavior of a sexual nature or any other behavior based on gender that affects the dignity of women and men at work. This includes, in particular, threats, promises of benefits, the imposition of coercion and the exertion of pressure to obtain sexual favors".

The enumerations in Article 4 paragraph 2 CH-GlG only refer to cases of abuse of power. However, the definition is not exhaustive and, according to the Swiss Federal Supreme Court's case law, covers all behavior that affects the dignity of the employee and contributes to the creation of a hostile working climate.[51] According to the Swiss Federal Supreme Court, sexual harassment can take various forms: sexist statements, use of pornographic material, embarrassing invitations, advances with promises of rewards or threats of reprisals, as well as inappropriate jokes. Ultimately, the definition covers all unwanted behavior of a sexual nature.[52] The individual act itself does not necessarily have to have a sexual reference, it is sufficient if this is apparent from the context.[53] Thus, as in German law, the form that sexual harassment can take is not limited.[54] The CH-GlG also requires that the act violates the dignity of the person concerned (Article 4).

3. Racist Discrimination in the Workspace

As laid out above, in Germany the AGG covers racist discrimination in the workspace in the same manner as sexual harassment. In Switzerland, the legislation on racist discrimination is fragmentary. The Swiss Constitution (Bundesverfassung) states in its Article 8 paragraph 2 that no one must be discriminated (inter alia) due to origin or race.[55] Article 261bis of the Swiss Criminal Code penalizes anyone who publicly incites racism and hatred with imprisonment of up to three years.[56] However, this rule is limited to especially severe racist discrimination in the public. No specific legislation comparable to the CH-GlG addresses discrimination on grounds of race in the workspace in Switzerland.

[49] BAG, 6/9/2011 – 2 AZR 323/10, Rn. 23; *Bauer/Krieger/Günther*, Allgemeines Gleichbehandlungsgesetz und Entgelttransparenzgesetz, 5. Aufl. 2018, § 3, Rn. 52.

[50] *Bauer/Krieger/Günther*, Allgemeines Gleichbehandlungsgesetz und Entgelttransparenzgesetz, 5. Aufl. 2018, § 3, Rn. 59 and Rn. 43.

[51] BGer 4A_105/2018 dated 10/10/2018, Erw. 4.2.1; BGer 4C.289/2006 dated 2/5/2007, Erw. 3.1, with reference to BGE 126 III 395, Erw. 7b/bb.

[52] BGer 4A_544/2018 dated 8/29/2019, Erw. 3.1 with further references.; BGer 4A_18/2018 dated 11/21/2018, Erw. 3.1 with further references.

[53] BGer 4A_544/2018 dated 8/29/2019, Erw. 7.2.

[54] *Kaufmann,* in: Kaufmann/Steiger-Sackmann (Hrsg.), Kommentar zum Gleichstellungsgesetz, 2. Aufl. 2009, Art. 4, Rn. 54.

[55] Bundesverfassung der Schweizerischen Eidgenossenschaft of April 18, 1999 (Effective July 1, 2020), SR 101.

[56] Schweizerisches Strafgesetzbeuch of December 21, 1937 (Effective July 1, 2020), SR 311.0.

4. Job Reference

In Germany and Switzerland, the legal regulations mentioned above only cover sexual harassment (and racist discrimination in Germany) in the context of a dependent employment relationship or in the case of the initiation of a self-employed employment relationship. [57] A necessary connection to the employment relationship is given if the discrimination occurs in the workspace. Outside working hours, a connection to the employment relationship is given if there is an operational connection.[58]

According to the view taken here, the workspace includes all premises and means of transport used in the course of the exercise of the profession (such as office buildings, external conference and seminar rooms, hotels, restaurants, railways, aircraft, taxis, etc.), including business trips, training events or celebrations organized by the employer (e.g. office or Christmas party), as well as the journey to and from these places.[59]

5. Discriminating Person

Discrimination in the workspace can be carried out internally by superiors, subordinates, colleagues or externally by third parties[60] such as customers, service providers, partner companies or suppliers.

6. Company definition of Sexual Harassment and Racial Discrimination

A literal reproduction of the above mentioned legal definitions is obviously not very suitable for a company's own code of conduct. These standards are too technical. Employees should be given a short and clear explanation of what is understood by sexual and racial discrimination in their own organization.

The starting point for a company's own definition of sexual harassment can be that sexual harassment in the workspace is understood as a particularly severe form of discrimination.[61] In addition, there is the basic understanding that sexual harassment can take many different forms: A first approach to differentiating between forms of sexual harassment is to differentiate between quid pro quo harassment and hostile working atmosphere. In the first case, the person concerned is specifically threatened with disadvantages in the employment relationship either if he or she rejects the sexual advances or if the expectations are fulfilled and advantages are promised. In the second case, a hostile

[57] *Bauer/Krieger/Günther*, Allgemeines Gleichbehandlungsgesetz und Entgelttransparenzgesetz, 5. Aufl. 2018, § 6, Rn. 4, 6; *Kaufmann,* in: Kaufmann/Steiger-Sackmann (Hrsg.), Kommentar zum Gleichstellungsgesetz, 2. Aufl. 2009, Art. 4, Rn. 65.

[58] *Köhler/Koops*, BB 2015, 2807, 2808; *Bauer/Krieger/Günther*, Allgemeines Gleichbehandlungsgesetz und Entgelttransparenzgesetz, 5. Aufl. 2018, § 3, Rn. 50; *Kaufmann,* in: Kaufmann/Steiger-Sackmann (Hrsg.), Kommentar zum Gleichstellungsgesetz, 2. Aufl. 2009, Art. 4, Rn. 64.

[59] *Schlachter*, NZA 2001, 121, 124; *Kaufmann,* in: Kaufmann/Steiger-Sackmann (Hrsg.), Kommentar zum Gleichstellungsgesetz, 2. Aufl. 2009, Art. 4, Rn. 64; *Tag*, Sexuelle Übergriffe in Betrieben, Unternehmen und Verwaltungen, in: Senn (Hrsg.), Diskriminierung – Wahrnehmung und Unterordnung, 2009, S. 35, 52 f; *Bauer/Krieger/Günther*, Allgemeines Gleichbehandlungsgesetz und Entgelttransparenzgesetz, 5. Aufl. 2018, § 3, Rn. 50.

[60] Section 12 Abs. 4 AGG.

[61] Former Swiss Federal Council member *Arnold Koller* described it as a "particularly degrading form of gender discrimination", AmtBull NR 1994 249.

working atmosphere is generally created.[62] However, sexual harassment is not limited to this and should be defined openly. Sexual harassment can manifest itself in particular (but not conclusively) by addressing physical characteristics, staring, unwanted intrusions, stalking, sexist language, jokes or allusions, gestures, obscene statements, unwanted sexual advances as well as sexual assaults, bullying, coercion, physical violence or threats of it up to and including rape.[63] The term sexual harassment also includes sexist behavior. This includes any behavior without sexual reference which discriminates against or degrades people on the basis of their sex.[64]

A possible definition for the company's own code of conduct could therefore be as follows: Sexual discrimination in the workspace is understood to be any behavior with a sexual connotation that is undesirable from one side and which violates a person's dignity.[65] By using the gender-neutral term "person", it is made clear that sexual assault, harassment and discrimination can affect women and men, as well as people with the gender entry “diverse”.

The decisive factor here should not be the motivation of the perpetrator, but the perception of the victim.[66] In our view, this is the only way to achieve effective protection of the person concerned. An objectification - and thus also a protection of the accused person against misunderstandings, hypersensitivity and abuse – is made by the second criterion, according to which the conduct must violate the dignity of a person.[67] The company's own definition can be supplemented by examples to make the non-tolerated behavior clearer to the employees.

Racist behavior in the workspace may take many forms. E.g. starting from discriminatory job advertisements, discriminatory preselection, discriminatory employment to discriminatory contract contents, discriminatory project assessment, and of course discriminatory behavior by racist speech or gestures.[68]

[62] *Kaufmann,* in: Kaufmann/Steiger-Sackmann (Hrsg.), Kommentar zum Gleichstellungsgesetz, 2. Aufl. 2009, Art. 4, Rn. 23.

[63] See also the listing in the guidance regarding Verordnung 3 zum Schweizerischen Arbeitsgesetz, SECO March 2014, 302 – F.

[64] *Tag*, Sexuelle Übergriffe in Betrieben, Unternehmen und Verwaltungen, in: Mischa Senn (Hrsg.) Diskriminierung – Wahrnehmung und Unterordnung, 2009, S. 35, 52. This is also the definition of the Federal Office for the Equality of Women and Men from January 2008. If unwanted advances are not reciprocated, the perpetrator's behavior can turn into bad-mouthing or mobbing of the resisting person, as happened in the described case in: Binswanger, „Zeig doch deine Assets ;-)“, Tagesanzeiger dated 12/11/2018, see https://www.tagesanzeiger.ch/wirtschaft, see https://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/zeig-doch-deine-assets/story/23578823.

[65] Based on the definition by the Federal Office for Gender Equality of January 2008; guideline on Verordnung 3 zum Schweizerischen Arbeitsgesetz of March 2014, 302 – G.

[66] Likewise, the definition of the Federal Office for Gender Equality from January 2008; Section 3 paragraph 4 AGG, which speaks of "undesirable" behavior.

[67] In our opinion, even the attempt is sufficient to trigger the examination of measures by the company. According to Section 3 paragraph 4 AGG, it is sufficient for sexual harassment to have occurred if an act is intended to violate the dignity of the person concerned.

[68] As with the definition of sexual harassment it makes sense to specify the organization's understanding of racist discrimination in its code of conduct.

B. Employer Obligations

1. Germany

The employer is obliged to actively protect its employees against discrimination, including sexual harassment and racist discrimination (Section 12 paragraph 1 in conjunction with Section 3 AGG). In doing so, the employer should take preventive measures to ensure that there is no discrimination in the workspace (Section 12 paragraph 2 AGG).[69] The employer can achieve this by indicating the inadmissibility of such discrimination in the context of initial and further vocational training and by ensuring that sexual and other harassment does not occur. The employer is not legally obliged to take these preventive measures and training courses. However, this does give him the possibility of exculpation (Section 12 paragraph 2, sentence 2 AGG). For if the employer violates the duty to protect his employees from such harassment, he is liable for damages in the event of prohibited discrimination (Section 15 AGG).[70]

Paragraph 3 of Section 12 AGG obliges the employer to intervene in the event of a violation by an employee and to put an end to the violation. This implicitly obliges the employer to investigate a reported violation internally or by a third party.[71] Only in this way can he determine whether a violation has actually occurred, who is involved in it and what the appropriate, necessary and reasonable measures are. Pursuant to Section 12 paragraph 4 AGG, the employer is obliged to take measures to protect employees from discrimination by third parties within the scope of their professional activities.

The employer is also explicitly obliged to follow up on any indications of discrimination and to inform the whistleblower of the result (Section 13 paragraph 1 AGG).[72]

2. Switzerland

In Switzerland, Article 328 of the Swiss Code of Obligations (CH-OR)[73], Article 6 of the Federal Law on Work in Industry, Trade and Commerce (CH-ArG)[74] and Article 3 to 5 CH-GlG are relevant to the employer's corresponding obligations.

Article 328 CH-OR sets out the employer's general duty of care to ensure the protection and health of employees. This results in a clear duty to act within the bounds of what is reasonable from an operational point of view, because the employer "must respect and protect the personality of the employee in the employment relationship, take due account of his or her health and ensure that morality is upheld. (...)". Article 328 paragraph 1 CH-OR subsequently explicitly emphasizes protection against sexual harassment: "(...) In particular, he [the employer] shall ensure that workers are not subjected to sexual harassment and that victims of sexual harassment do not suffer further

[69] *Bauer/Krieger/Günther*, Allgemeines Gleichbehandlungsgesetz und Entgelttransparenzgesetz, 5. Aufl. 2018, § 4, Rn. 4.

[70] For details of the prevention measures, see section V.

[71] *Bauer/Krieger/Günther*, Allgemeines Gleichbehandlungsgesetz und Entgelttransparenzgesetz, 5. Aufl. 2018, § 12, Rn. 30.

[72] Finally, the employer is prohibited from taking repressive measures against the employee concerned, his or her supporters and witnesses (Section 16 Abs. 1 AGG).

[73] Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuchs (Fünfter Teil, Obligationenrecht) dated 3/30/1911 (Effictive: 1.4.2020), SR 200.

[74] Bundesgesetz über die Arbeit zu Industrie, Gewerbe und Handel (Arbeitsgesetz) dated 12/9/2018, SR 822.11.

disadvantages. This duty of care thus also includes prevention, acute protection in the event of an incident (such as immediate and long-term measures) and protection against repression.[75] The employer's obligation pursuant to Article 328 CH-OR comprises all aspects of discrimination, including on grounds of origin or race.[76]

In addition, the CH-GlG prohibits in Article 3 in conjunction with Article 4 the sexual harassment of employees as a special case of the general prohibition of discrimination. It does not impose any further explicit legal obligations on the employer. However, in Article 5 paragraph 3 CH-GlG, the law grants the employee concerned a right to compensation if employers cannot prove that "they have taken measures which are necessary and appropriate to prevent sexual harassment according to experience and which can reasonably be expected of them". The employer is thus liable if he has not taken sufficient and reasonable preventive measures.[77] In our view, this should also apply if the employer, following an established case of harassment, does not take reasonable and appropriate measures to prevent continuing harassment.[78]

Finally, Article 6 paragraph 1 of the CH-ArG stipulates that the employer "(...) shall take the necessary measures to protect the personal integrity of the employees". This protection corresponds to the protection of personality according to Article 328 CH-OR. The provisions of public employment law reinforce this effect.[79]

3. Conclusion

Employers in Switzerland as well as in Germany are legally obliged to protect their employees from discrimination, including sexual harassment and racist behavior by other employees or third parties in their workspace.

Prevention is not mandatory by law. However, employers are strongly recommended to do so - if only for the basic idea of the duty of protection towards employees, for the idea of treating the risk of discrimination equally with other compliance risks, and in order to preserve the possibility to exculpate oneself in accordance with legal requirements.

Employers in Germany and Switzerland, on the other hand, are legally obliged to appropriately investigate any indication of sexual harassment and other discrimination, to clarify the facts of the case (as far as possible) and to take measures to prevent further harassment. This also includes taking immediate measures in the event of further harassment.

[75] *Ulrich*, Sicherheit & Recht 2014, 223, 225.

[76] See https://www.rechtsratgeber-frb.admin.ch/lebensbereiche/d101.html.

[77] *Kaufmann,* in: Kaufmann/Steiger-Sackmann (Hrsg.), Kommentar zum Gleichstellungsgesetz, 2. Aufl. 2009, Art. 4, Rn. 52.

[78] In case of sexual harassment, in addition to compensation (Article 328 CH-OR) and satisfaction (Article 49 CH-OR), the person concerned may claim compensation for lack of prevention in the amount of up to six average monthly Swiss wages (Article 5 paragraph 3 CH-GlG), should the employer not be able to exculpate himself. Such an exculpation is not available if the employer himself commits the sexual harassment; *Kaufmann,* in: Kaufmann/Steiger-Sackmann (Hrsg.), Kommentar zum Gleichstellungsgesetz, 2. Aufl. 2009, Art. 4, Rn. 55.

[79] Wegleitung zum Arbeitsgesetz, Article 6, SECO, November 2006, 006-2.

IV. VALUES OF AN ORGANIZATION

A value-based corporate culture describes a culture in which an organization aligns its decisions and actions internally and externally with the corporate values it has laid down.[80]

Organizations for which such corporate values are more than just lip service also align their CMS to adhere to the corporate values. In order to give these corporate values a meaning that can be lived and experienced and to allow identification with these values, they should be explained and defined.

It is advisable not to let the values be determined by the management alone, but to involve (selected) employees.

Clearly formulated corporate values provide employees with basic orientation, especially in complex situations, and thus help them to make stringent and comprehensible decisions. This also applies to conflict situations among employees on a personal level. Whether behavior towards colleagues in the workspace is tolerable can also be measured by corporate values such as "respectful" or "appreciative" treatment.

V. INTEGRATION OF SEXUAL DISCRIMINATION CASES INTO A VALUE-BASED COMPLIANCE MANAGEMENT SYSTEM

The approach to and management of the risk of sexual, racist and other discrimination in the workspace can be well integrated into existing CMS, taking into account specific aspects. When setting up new CMS, it is advisable to incorporate the handling of discrimination incidents from the outset.

A. Preventive measures to protect against sexual harassment, racist and other discrimination

One of the aims of CMS is prevention. This includes measures to mitigate compliance risks.[81] Organizations may implement various preventive measures to protect against sexual harassment, racist and other discrimination, which have varying degrees of effectiveness. The typical measures vary in particular between fact sheets, internal company policies, general compliance training and codes of conduct. However, these measures often do not lead to the desired goal: according to the 2019 IBA Study, employees in workspaces with policies and training are as likely to become victims of discrimination as employees in workspaces without such measures.[82]

There is a need for further measures that go beyond this and clearly address, in particular, the following aspects: Raising awareness, reviewing and implementing anti-discrimination policies and

[80] In-depth see *Grüninger*, in: Wieland/Steinmeyer/Grüninger (Hrsg.), Handbuch Compliance Management, 2. Aufl. 2014, S. 41, 52 et seq.

[81] *Grüninger*, in: Wieland/Steimeyer/Grüninger (Hrsg.), Handbuch Compliance-Management, 2. Aufl. 2014, S. 41, 60, Rz. 24.

[82] *Pender*, Us Too?, Bullying and Sexual Harassment in the Legal Profession, International Bar Association, May 2019, see https://www.ibanet.org/bullying-and-sexual-harassment.aspx, p. 8.

standards, introducing regular, tailor-made training on discrimination in the workspace, taking responsibility, collecting data and improving transparency.[83]

1. Corporate Culture

One of the most important preventive measures a company can take is to establish and live a corporate culture in which all employees are safe from discrimination. A prerequisite for this is the living of this culture by the management ("tone from the top"). Mindfulness is a key aspect of such a corporate culture. This means that it is part of the duty of care of the employer and its managers to look and act responsibly in the event of discrimination. Because "looking away is looking on, and looking on is enabling: Structural abuse of power does not mean that everyone acts abusively, but that the structures tolerate those who do not".[84]

The basis for this is (repeated) communication to employees and other stakeholders [85] that discrimination and, in particular, sexual harassment or racist behavior will not be tolerated by the employer and will be consistently sanctioned. This alone has a deterrent effect. It also includes informing employees and other stakeholders about how the company defines such different types of discrimination. After all, unclear circumstances are an invitation to infringements.[86] According to the authors, it is also important that this communication is made by the top management of the company so that the topic is understood as correspondingly serious and important.

The implementation of such a corporate culture and the corresponding communication is often accompanied by the concern that (especially anonymous) reports encourage the misuse of a whistleblower system. For this reason, it must also be made clear in the communication that an abusive report also constitutes misconduct and will be sanctioned accordingly.

In the authors' view, consistent action in this context means that any credible report of discrimination must be investigated and, in the event of a proven violation, sanctioned. This should apply without exception, regardless of the hierarchical positions of the persons involved. In the context of sexual harassment, this is particularly important as it often occurs in connection with abuse of power. As in compliance incidents of other categories, employees only trust the CMS if they see that they are implemented. And only in this case do they function preventively.

2. Diversity & Inclusion

A corporate culture of mutual respect and esteem, irrespective of a person's personality traits, can be created in particular through diversity and inclusion measures. The authors understand the term "diversity" to mean the active identification of existing diversity within the company and the creation of the desired diversity. "Inclusion" stands for the efficient linking of this diversity into productive and innovative units. The economic benefits of inclusion can only be realized in an environment of mutual

[83] *Pender*, Us Too?, Bullying and Sexual Harassment in the Legal Profession, International Bar Association, May 2019, see https://www.ibanet.org/bullying-and-sexual-harassment.aspx, p. 8.

[84] *Petersen*, Einzelfälle? Strukturwandel? Zivilcourage?, Hochparterre dated 2/20/2019, see https://www.hochparterre.ch/nachrichten/architektur/blog/post/detail/einzelfaelle-strukturwandel-zivilcourage/1550606879/.

[85] This includes third parties (such as service providers and customers) and investors.

[86] Wegleitung zur Verordnung 3 zum Arbeitsgesetz, SECO March 2014, 302-H.

respect and appreciation. The required respect also operates as a preventive measure against sexual harassment and other discrimination.

Measures to create diversity and inclusion in companies are diverse and individual. A fundamental element is the sensitization of employees and management to their own unconscious bias. Building on this, measures can be taken to raise awareness of the existing diversity and the diversity that needs to be expanded, to reduce fears and to demonstrate the possibility of personal involvement in promoting diversity and inclusion in the company.

Diversity and inclusion measures can also be effectively demanded by business partners. In early 2020, Novartis announced that it will only hire law firms that meet fixed diversity benchmarks: at least 30% of billable associate and 20% of partner time must be provided by women, ethnically diverse lawyers or lawyers belonging to the LGBTQ+ community. [87]

3. Specific Training

It is questionable whether general compliance training meets the requirements for prevention or training in Section 12 paragraph 2 sentence 1 AGG or Article 5 paragraph 3 CH-GlG.[88] The 2019 IBA Study shows that mere guidelines and training do not seem to have the desired effect. Employees in companies with such measures become victims of sexual harassment to the same extent as employees in companies without such measures.[89]

On the other hand, according to the US study by *Johnsons/Keplinger/Kirk/Barnes*, specific training on sexual harassment, microaggression and unconscious bias can not only encourage civil behavior but also enable colleagues and managers to intervene when they see bullying or harassment in the workspace.[90] Because "racism isn't biological, bias is".[91]

One promising and simple measure is to empower employees to actively intervene and resolve an acute discrimination situation. According to the *Johnsons/Keplinger/Kirk/Barnes* study, these efforts are most successful when - in the case of harassment of women - organizations successfully involve male allies in the discussion on gender equality.[92] With the ability to defend themselves and with the support of allied colleagues, the number of investigations, e.g. inappropriate remarks, could also be reduced. It is also more likely to enable the staff concerned to work constructively together again after a clarifying discussion than if an official internal investigation is conducted to this end.

[87] Press release dated 2/12/2020 see https://www.novartis.com/news/novartis-preferred-firm-program-legal-services-launched.

[88] See also *Köhler/Koops*, BB 2015, 2807, 2810, Fn. 47.

[89] *Pender*, Us Too?, Bullying and Sexual Harassment in the Legal Profession, International Bar Association, May 2019, see https://www.ibanet.org/bullying-and-sexual-harassment.aspx, p. 8.

[90] *Johnson u. a.,* Has Sexual Harassment at Work Decreased Since #MeeToo?, Harvard Business Review 7/18/2019, see https://hbr.org/2019/07/has-sexual-harassment-at-work-decreased-since-metoo.

[91] *Khalil Smith/David Rock*, 3 Reasons why "Anti-Bias" may solve more than "Anti-Racism", Forbes, 9/18/2020.

[92] *Johnson u. a.,* Has Sexual Harassment at Work Decreased Since #MeeToo?, Harvard Business Review 7/18/2019, see https://hbr.org/2019/07/has-sexual-harassment-at-work-decreased-since-metoo.

4. Procedure for Dealing with Acute Incidents

Despite optimal prevention, sexual harassment and other discrimination in the workspace cannot be completely prevented. Accordingly, as part of prevention, organizations should have standardized and implemented their processes for dealing with acute incidents in the same way as they do with regard to other compliance risks. In particular, this includes defining responsibilities and ensuring that the process can run without conflicts of interest.[93] This prevents, for example, the bizarre situations where management itself investigates allegations of sexual harassment against management and thus fails to provide evidence of exculpation.[94]

B. Contact Person and Whistleblower System

Depending on its size the organization may offer its employees a contact person for discrimination incidents. This is an offer by the organization to have a trained contact person available who can provide competent assistance and initiate appropriate processes. However, it is not enough to have this contact person present. It is just as important that employees are aware of this person because, according to the study by the German Federal Anti-Discrimination Agency (Antidiskriminierungsstelle des Bundes), one third of those questioned are unaware of the existence of a contact person.[95] It is known from various cases that victims did not know who to turn to.[96] In order to successfully establish such role the organization should repeatedly and positively communicate such role to its employees.

In addition to or as an alternative to the contact person, a reporting office for information can be set up, to which employees can send their report of a violation, even anonymously. These reporting offices are the whistleblower systems to be provided according to the EU Whistleblower Directive[97], which also guarantees protection to the whistleblower. In Switzerland there is currently no legal protection for whistleblowers.[98] It is advisable to standardize the reporting of discrimination cases and the subsequent procedure.

Simply making reporting points available does not necessarily mean that misconduct can be identified early on: For example, according to the 2019 IBA study, three-quarters of harassed persons have not reported bullying or sexual harassment even in sectors such as legal advice. The surveyed persons mentioned the status of the harasser, fear of the consequences of a report and the endemic nature of such incidents in law firms as reasons for not reporting.[99] This shows that a company must first win the trust of its employees. Employees must be confident that their report will be treated confidentially, a

[93] See section VI.B.

[94] BGE 126 III 395, Erw. c).

[95] Studie der Antidiskriminierungsstelle des Bundes, Sexuelle Belästigung am Arbeitsplatz dated 3/3/2015, see https://www.antidiskriminierungsstelle.de/SharedDocs/Downloads/DE/publikationen/Umfragen/Handout_Umfrage_sex_Belaestigung_am_ArbPlatz_Beschaeftigte.pdf;jsessionid=31664677A3430789E110157E2DEC7EE5.2_cid340?__blob=publicationFile&v=4.

[96] *Honegger*, Nach Sex-Vorwürfen an der Uni Basel: Umstrittener Dozent kehrt zurück, BZ dated 9/14/2019, see https://www.bzbasel.ch/basel/basel-stadt/nach-sex-vorwuerfen-an-der-uni-basel-umstrittener-dozent-kehrt-zurueck-135618864.

[97] 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, PE/78/2019/REV/1 ABl. L 305 dated 11/26/2019, S. 17–56.

[98] See *Pikó*, CB 2019, 235-242; Pikó, Swiss Legal Status on the Protection of Whistleblower, CEJ (6) 2020, p. 32 – 50.

[99] *Pender*, US Too?, Bullying and Sexual Harassment in the Legal Profession, International Bar Association, May 2019, p. 8, see https://www.ibanet.org/bullying-and-sexual-harassment.aspx.

legitimate report will not trigger reprisals, the company will fulfil its duty of investigation - regardless of the status of the people involved - and that the company will sanction the harasser appropriately.

C. Risk Analysis

The risks of discrimination, in particular sexual harassment and racist behavior, must also be seriously evaluated as part of the regular internal compliance risk analysis.

Such cases may be categorized according to whether they are already known to the company and have been dealt with legally, those that are already known but have not yet been dealt with legally and finally those that are unknown to the employer.[100] But be careful: the mere absence of reported cases should not be taken as a lack of discrimination incidents. The reason for such absence may be that the whistleblower system does not exist, does not work, employees are not aware of the reporting possibilities, they do not trust the whistleblower system or are simply afraid or ashamed to talk about the incident.[101]

Furthermore, as with any risk analysis, the risks must be qualified according to the probability of occurrence and potential damage.

D. Data Collection

In order to be able to assess measures taken and existing or future risks with regard to discrimination in the organization, data should be collected within the limits of data protection laws. For example, it is worth considering compiling anonymous statistics on the cases that have occurred in order to identify possible patterns at an early stage. Such data can also be used to draw conclusions about the efficiency of internal investigations.

E. Transparency

Transparency is a difficult point to communicate in relation to discrimination in the workspace, in particular, when it comes to sexual harassment. No company wants to be associated with such behavior. If one follows the statistics mentioned at the beginning, one cannot help but accept that sexual harassment (like other forms of discrimination) will occur over time in any larger (and perhaps smaller) company. Against this background, it is important to consider how proactively this issue can be dealt with. Regular factual information of employees about investigated and sanctioned compliance incidents (including discrimination) can have positive effects: employees (and other stakeholders) can conclude that the company not only communicates but also acts on reported discrimination. Employees are made aware that violations have consequences and that reports are investigated. This transparency can thus contribute to prevention as well as to early detection of risks of sexual, racist and other discrimination in the organization.

[100] Corresponding to *Balthasar-Wach/Hofbauer*, juridikum 2019, 326, 331.

[101] In addition, non-disclosure agreements, usually with monetary payments to the employee concerned, may also explain the absence of reports.

VI. INTERNAL INVESTIGATIONS ON SEXUAL ASSAULT AND OTHER DISCRIMINATION CASES

A. Aim of the Internal Investigation

As explained above[102], the employer is legally obliged or at least incentivized to investigate the report of a discrimination incident in the organization. If there is reasonable suspicion, the employer is obliged to take measures; in particular, the employer must immediately protect the employees concerned from further disadvantages and take action against further harassment. The conduct of an internal investigation is suitable for this purpose.[103] The internal investigation may relate to both current and past cases. According to a study, 23 percent of the German employers surveyed in response to #MeToo have reopened previous investigations of sexual harassment.[104]

The aim of an internal investigation is to establish the facts of the case and, if misconduct has been established, to identify the persons responsible for it. Properly conducted internal investigations also have a preventive effect. Finally, they contribute to the improvement of existing processes in the remediation phase. These principles apply to all compliance violations. Investigations of discrimination cases, in addition, show some special features which are dealt with below.

First of all, the following decisive difference should be mentioned: In contrast to compliance incidents of a white-collar criminal nature (such as fraud, corruption and competition agreements), sexual harassment, racist and other discrimination incidents involve a victim who is personally affected in his or her private or intimate sphere. While economic compliance incidents are mainly about the identification of the persons involved and the determination of the extent of the damage,[105] in case of sexual harassment or racist discrimination it is equally important to protect and take care of the victim.

B. Receipt of a Report on a Discrimination Incident

In the vast majority of cases, an internal investigation is opened on the basis of a report of a discrimination incident. This may be on the basis of personal discussions with compliance staff, e-mail or the whistleblower reporting systems. Sources can be own employees, business partners, the persons concerned or media reports. The whistleblower may be a witness or a person directly or indirectly affected.

Responsibility for investigating a compliance incident related to discrimination allegations may lie with the Compliance Department, a separate Internal Investigations Department or other internal departments within the organization, such as HR, Internal Audit or Legal. It is a particular challenge for members of HR departments to conduct internal investigations if they remain involved in HR activities.

---

[102] See section III.

[103] As far as can be seen at present, the draft Verbandssanktionsgesetz (VerSanG) shall only apply to cases of white-collar crime: The VerSanG is to regulate the sanctioning of associations for criminal offences by which obligations affecting the association have been violated or by which the association has been or should be enriched (Section 1 VerSanG). Whether and to what extent regulations of the VerSanG on internal investigations should also be applicable to those in connection with sexual harassment or other discrimination cases is not clear at present.

[104] *Littler*, press release dated 11/12/2018, New Littler Research Reveals 79% of European Employers are Taking Action to Reduce Risks of Sexual Harassment, see https://www.littler.com/publication-press/press/new-littler-research-reveals-79-european-employers-are-taking-action-reduce.

[105] And, depending on the circumstances, additionally cooperation with the investigating authorities.

This is because they have many points of contact with employees and must continue to work with their colleagues even after the investigation has been completed.

It must be ensured that the investigators do not have a conflict of interest. This may be challenging, especially if the company is medium-sized or small and has a limited number of employees. Or if an executive or other person important to the company (e.g. a key customer) is involved. It is irrelevant to the effectiveness of the investigation whether the conflict of interest actually affects the investigation. Even the (justified) appearance of a conflict of interest can have a fatal effect on the investigation. If employees or other stakeholders get the impression that the investigation process is not conducted fairly, any preventive effect is lost. It can also act as a deterrent to future reports and generally demotivate employees.

It is essential that confidentiality is maintained for both the person concerned and the accused. Careful consideration must be given to those who may have knowledge of the incident in order to protect the personal rights of both the person concerned and the accused.[106] This must always be considered when selecting, possibly questioning and involving witnesses, employees, translators, superiors etc. in the course of the investigation. If necessary, this is to be further secured by confidentiality agreements, even if confidentiality regulations should exist in a code of conduct.

C. Triage

The department designated as responsible for reported discrimination must carry out a triage immediately upon receipt of the notification. Triage is used to decide whether or not to open an investigation and to determine the priority of the investigation. Decision criteria for triage can be the nature and severity of the offence, the frequency of the misconduct, organizational factors favoring the misconduct as well as the position and hierarchical status of the persons involved.[107]

When triage of discrimination cases is carried out, it is recommendable to divide the reports into categories, e.g. three priority levels. The first priority typically includes serious incidents as well as incidents involving persons with a senior management function (and thus a corresponding responsibility and role model function). Cases which do not belong to the first and third priority levels have second priority. The third priority includes cases that do not qualify as compliance violations.[108]

The importance of this triage is shown by the cases of sexual harassment taken up by the media, whose internal investigations had to be repeated due to a lack of initial examination. This also has an impact on the reputation of the organization and the trust that employees place in the organization.[109] When in doubt, therefore, one should not look away, but rather take a close look right from the start.

[106] *Fritsche*, Interne Untersuchungen in der Schweiz, Zürich/St. Gallen, 2013, p. 67 f.

[107] Comparable to OCEG Anticorruption Illustrated Series, see https://go.oceg.org/illustration-ac-part-5-how-to-conduct-investigations-of-corruption.

[108] These include, for example, employee suggestions for improvements, general HR concerns or misguided communications.

[109] For example in the case described by *Binswanger/ Alich*, #MeToo bei EY: Kadermann per sofort freigestellt, Tagesanzeiger dated 12/14/2018, see https://www.tagesanzeiger.ch/wirtschaft/standardey-stellt-mitarbeiter-nach-vorwuerfen-per-sofort-frei/story/22803713.

D. Emergency Measures and Initiation of Proceedings

If the triage decision is to carry out an internal investigation, the next step is to consider emergency measures. Particularly in the case of indications of sexual harassment, speed is required on the one hand and sensitivity and a sense of proportion on the other. The employer is required to find the right balance between protecting the victim from further harassment and protecting the accused person from false accusations. Depending on the severity of the incident, physical separation of the involved persons may be required. Further cooperation between the persons involved may also have to be suspended until further notice. Possible immediate measures can be, in particular, a temporary transfer to another location or to the home office, a paid temporary leave of absence or the official order to take accumulated leave. In the case of sexual assaults in particular, an official order to stay away from the persons affected or involved until the investigation is concluded can also be considered.

An important aspect is the decision whether the internal investigation should be conducted by the company's own employees or by external persons. In particular, the following reasons may speak in favor of an investigation by external persons: The internally responsible persons lack the specific training to conduct such an investigation of sexual harassment incidents, there is a lack of internal capacities for a quick and efficient investigation or management personnel are involved.[110] It is particularly in cases of sexual discrimination that system-immanent difficulties repeatedly arise. For example, if a newly appointed head of HR's first official act is to investigate against the superior who recruited him.[111]

In the phase of initiating proceedings, the investigating team has to decide on the subject of the investigation and determine the investigative measures. In the context of discrimination cases, the main focus is on interviewing witnesses, colleagues and persons involved.

E. Accompanying the Harassed Person

In contrast to investigations of white-collar crime, the employer is required to ensure the protection and welfare of the person concerned. First of all, the investigating team should always be aware of how much of an effort was required from the harassed person to report the incident or talk about it.

Many cases of sexual discrimination or even rape are not reported at all[112] or only years after the incident due to fear. The actress and director *Asia Argento* expressed what she was afraid of: *Weinstein*

[110] Today, the attorney-client privilege probably plays a rather minor role in this question, since according to case law informal private interviews by attorneys are only protected by the attorney-client privilege to a limited extent. See for Switzerland: BGer, 9/26/2016 – 1B_85/2016 and for Germany: LG Hamburg, 10/15/2010 – 608 Qs 18/10; LG Mannheim, 3.7.2012 – 24 Qs 1/12, 24 Qs 2/12; LG Braunschweig, 21.7.2015 – 6 Qs 116/15.

[111] *Binswanger*, Der Fehler liegt im System, Nulltoleranz-Politik bei sexueller Belästigung ist bei vielen Firmen bloss ein Lippenbekenntnis, Tagesanzeiger dated 12/12/2018, see https://www.tagesanzeiger.ch/schweiz/standard/der-fehler-liegt-im-system/story/14786255.

[112] See, for example,. *Pender*, Us Too?, Bullying and Sexual Harassment in the Legal Profession, International Bar Association, May 2019, p. 8; pursuant to which 75% of sexual harassment incidents are not reported by lawyers, see https://www.ibanet.org/bullying-and-sexual-harassment.aspx.

would destroy her career.[113] The persons concerned describe anger, insult, degradation, powerlessness, disappointment, isolation, loneliness and above all shame.[114]

In her book, *Chanel Miller* has described in detail the ordeal for the affected person of having to repeat the incident over and over again in several places and over a long period of time.[115] Therefore, it is the responsibility of the investigation team to spare the person concerned from this by good planning and questioning. For the same reason, internal investigations should not be prolonged. For example, a procedure that takes more than six months can lead to a severe strain on the person concerned.[116] The interview should always be conducted by two persons of different sex. Depending on the incident, the employer's offer of psychological support may also be an appropriate response for the person concerned.

F. Obligations of care towards the Accused Person

Usually, the harassed person is questioned prior to the accused person. The employer, however, also has duties of protection and care towards the accused person pursuant to Section 241 paragraph 2 German Civil Code. During the internal investigation, the accused person may not be subjected to unreasonable investigations, so that the employer's repressive measures must comply with the standard of Section 12 paragraph 3 AGG, and may not be disproportionate for the latter.[117] The same must apply in Switzerland under the employer's general duty of care pursuant to Article 328 paragraph 1 sentence 1 CH-OR.

G. Interrogation

In Germany, the employee's obligation to provide information is recognized as a secondary obligation arising from the employment relationship.[118] In Switzerland, the duty of loyalty of employees includes, among other things, the duty to avert damage to assets and reputation of the employer and the associated obligation to provide information and notification.[119] Employees are obliged to inform the employer unsolicited, truthfully, completely and in good time about all findings concerning possible grievances, disturbances, dangers or cases of damage.[120]

When questioning the person accused of discriminatory behavior, certain instructions must be given. These include, among other things, information on logging, confidentiality, obligation to provide

[113] *Farrow*, Catch and Kill, Lies, Spies and a conspiracy to protect predators, New York 2019, S. 247.

[114] *Rau*, Sie wirft Professor Übergriffe vor – und fühlt sich nun abgekanzelt, Tagesanzeiger dated 12/18/2019, see https://www.tagesanzeiger.ch/schweiz/standard/was-darf-eine-betroffene-nach-einem-missbrauchsfall-erwarten/story/30203736.

[115] *Miller*, Know My Name, New York 2019.

[116] *Rau*, Sie wirft Professor Übergriffe vor – und fühlt sich nun abgekanzelt, Tagesanzeiger dated 12/18/2019, see https://www.tagesanzeiger.ch/schweiz/standard/was-darf-eine-betroffene-nach-einem-missbrauchsfall-erwarten/story/30203736.

[117] *Krieger/Deckers*, NZA 2018, 1161, 1162.

[118] *Weiße*, in: Moosmayer/ Hartwig (Hrsg.), Interne Untersuchungen, 2012, S. 50; BAG, 6/23/1999 – 2 AZR 606/08, BB-Rechtsprechungsreport *Lipinski/Kumm*, BB 2010, 2444.

[119] *Wantz/Licci*, jusletter dated 2/18/2019, 5 f.

[120] *Streiff/von Kaenel/Rudolph*, Arbeitsvertrag, Praxiskommentar zu Article 319-362 OR, 7. Aufl. 2012, Article 321a OR, N 7.

information and possible rights to refuse to provide information.[121] The instructions also depend on who is conducting the internal investigation. If external lawyers conduct the internal investigation, they should inform the questioned person that they represent the employer's interests (so-called "Upjohn" or "Miranda" warning).[122]

In particular, the accused person must be fully informed about the allegations. It must also be examined whether the circumstances permit or make it recommendable that the accused person be accompanied by his or her own lawyer.

Depending on the circumstances, the internal investigation of the discriminatory incident must be extended to include evidence such as telephone data, email history, Internet use, etc. In this respect the limits of data protection law must be observed. A particular challenge is the examination of emails or other messages marked as private, which could contain discriminatory elements and are located on servers or terminal equipment of the employer. In this case, it must be clarified in advance what legal access the employer has. This depends on the specific circumstances, e.g. what is agreed in the employment contract provision on the use of the electronic equipment, whether there is effective consent or whether there is an overriding interest of the employer.[123]

H. Consequences and Sanctions against the Discriminating Person

If the internal investigation confirms the reported discriminatory behavior, the employer must draw the appropriate conclusions. The employer must take the appropriate, necessary and reasonable measures to stop the discrimination in the individual case, such as written warning, relocation, transfer or termination.[124]

Here too, special attention must be paid to the person concerned and it must be ensured that the person concerned (and all other employees) is safe from further harassment. The question of whether and how future cooperation between the person concerned and the discriminating person should take place must also be specifically addressed, in particular, in cases of sexual harassment. Here the employer may have to consider accompanying or further measures, such as a change of job, a transfer or a termination. And above all, it must be decided who these measures will affect: The person affected or the discriminating person. This may be a decision based on ethical, business or other criteria ideally defined by the organization in advance.

The employer can (and in principle must) issue an extraordinary dismissal in the case of an established case of discrimination if there is no other reasonable way to continue the employment relationship because all milder possibilities are unreasonable for the employer.[125] In contrast, an extraordinary

[121] *Fritsche*, Interne Untersuchungen in der Schweiz, Zürich/St. Gallen 2013, S. 173 ff u. 196 f.; *Wantz/Licci*, jusletter dated 2/18/2019, 26 et seq.; *Weiße*, in: Moosmayer/Hartwig (Hrsg.), Interne Untersuchungen, 2012, S. 53. The application of the nemo-tenetur principle to interviews in internal investigations remains controversial.

[122] *Bloch/Gütling*, SZW 2019, 275, 280.

[123] At least for Switzerland: *Wantz/Licci*, jusletter dated 2/18/2019, 18 et seq.

[124] See regarding the potential labour law consequences: *Krieger/Deckers*, NZA 2018, 1161, 1164 et seq.

[125] BAG, 2.3.2017 – 2 AZR 698/15; BAG, 6/29/2017 – 2 AZR 302/16; Article 337 CH-OR, according to which "good cause is defined as, in particular, any circumstance, the existence of which renders it unreasonable to expect the person giving notice to continue the

dismissal is not possible under German law if there is a more lenient means of action, such as a written warning, transfer or ordinary dismissal, which also achieves the purpose pursued by an extraordinary dismissal - not the sanction of conduct in breach of duty, but the avoidance of the risk of future disruption of the employment relationship.[126] Also in case of an ordinary termination due to discriminatory conduct there must be appropriate grounds, as otherwise the employee may claim to continue the employment.[127]

An important principle of labor law in Switzerland is the freedom of dismissal.[128] Employers and employees are in principle free to enter into and terminate an employment relationship. This freedom of termination is limited if the ordinary termination is due to abusive motives or if the employee is terminated without notice without good cause.[129] However, there is a fundamental difference to German labor law in this respect: In Switzerland, even an abusive ordinary termination or an unfounded termination without notice generally leads to the termination of the employment relationship. In this case, an employee who has been dismissed without notice in an abusive manner or without good cause can (only) claim compensation, but cannot demand reinstatement or continuation of the employment relationship.[130] There is a major exception to this rule in the context of Article 10 CH-GlG[131]: If an employee has filed an internal complaint of discrimination on grounds of his or her gender (including sexual harassment under Article 4 in conjunction with Article 3 CH-GlG) and such employee is subsequently dismissed without good cause[132], the employee may contest the dismissal. If the challenge is successful, the notice of termination is invalid and the employee must continue to be employed. The employee is protected against a new termination during the proceedings to contest the termination and for six months after the conclusion of the proceedings

employment relationship in good faith". This is likely to be the case, in particular, if sexual "harassment" qualifies as a serious criminal offence within the meaning of the criminal code.

[126] BAG, 6/29/2017 – 2 AZR 302/16, Rn. 27.

[127] The German Employment Protection Act (Kündigungsschutzgesetz), where applicable, aims to protect employees against so-called "socially unjustified dismissals" (Section 1 of the German Employment Protection Act, KSchG). Accordingly, a dismissal is only socially justified if it is based on reasons which (1) lie in the person of the employee or (2) in the employee's conduct or (3) are due to urgent operational requirements (Section 1, paragraph 2, KSchG). A further condition is, inter alia, that it is not possible to continue employment at a different workplace, under changed working conditions or after reasonable retraining or further training measures (section 1, paragraph 2, sentence 2, no. 1 b) and section 1, paragraph 2, sentence 3 of the KSchG).

[128] The following explanations are limited to employment relationships under private law. Employment relationships under public law as well as regulations from collective labor agreements (Gesamtarbeitsverträge, GAV) or normal employment contracts (Normalarbeitsverträge, NAV) are not dealt with.

[129] Article 336 CH-OR regarding abusive ordinary termination and Article 337c CH-OR regarding termination without notice without good cause.

[130] In the event of wrongful ordinary termination, the compensation corresponds to an amount of up to six months' salary (Art 336a paragraph 2 CH-OR). In the event of unjustified termination without notice, the employee is entitled to compensation for what he or she would have earned if the employment relationship had been terminated by observing the period of notice or, in the case of a fixed-term employment relationship, by expiration (Article 337c paragraph 1 CH-OR). In addition, the judge may award the employee a compensation amounting to a maximum of six months' wages (Article 337c paragraph 3 CH-OR).

[131] Article 10 CH-GlG is a special case which is covered by Article 366 paragraph 1 d. CH-OR. Accordingly, a notice of termination is abusive if the "other party asserts claims arising from the employment relationship in good faith".

[132] See in respect of Article 10 Rz. 14 ff *Riemer-Kafka/Ueberschlag,* in: Kaufmann/Steiger-Sackmann (Hrsg.), Kommentar zum Gleichstellungsgesetz, 2. Aufl. 2009, Art. 10 Rn. 14 et seq.

(Article 10 CH-GlG).[133] The purpose of Article 10 CH-GlG is to protect a complaining employee from a revenge termination by the employer.[134]

I. Remediation

Once the internal investigation has been completed, the final report should be analyzed with a view to subsequent remediation. This should include a root cause analysis and process review. Critical questions are to be asked, the answers to which may have an impact on the CMS and internal control systems (ICS). For example, the following may be reviewed: whether there were any warnings or complaints about the person causing the discrimination in advance, what the general working climate in the affected department is like, whether preventive measures have been taken and, if so, why these have not worked. Similarly, for example, the process of internal investigation can also be checked for efficiency.

VII. CONCLUSION

Cases of sexual harassment, racism and other discrimination are compliance incidents that are to be classified as serious compliance risks. Even if a compensation payment in the case of sexual discrimination and other discriminatory incidents in Switzerland or Germany is far from equal to the payments made in the USA, damage to the reputation of the organization and the associated loss of customers or employees can nevertheless be drastic. Organizations should therefore review and adjust their compliance management systems and processes to ensure that such risks can be professionally identified and managed. In comparison to white-collar crime, it should be noted that sexual and other discrimination always involves an employee who is personally affected in his or her private or intimate sphere. This is where the employer has a special duty of care. In addition, appropriate specific precautions must be taken for internal investigations.

[133] Another exception to the freedom of dismissal under Swiss law is that the employer cannot lawfully dismiss the employee during the so-called retention period. Blocking periods apply, among other things, to the performance of Swiss compulsory military or protection service or Swiss civilian service, in the event of illness or accident through no own fault or in the event of pregnancy (Article 336c CH-OR).

[134] See in respect of Article 10, Rz. 1. *Riemer-Kafka/ Ueberschlag* in: Kaufmann/ Steiger-Sackmann (Hrsg.), Kommentar zum Gleichstellungsgesetz, 2. Aufl. 2009, Art. 10, Rn. 1.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

IRAN, RUSSIA, CHINA: WHO'S NEXT?

U.S. EXPORT CONTROLS AND ITS EXTRA-TERRITORIAL APPLICATION

Philip Haellmigk

AUTHOR

Professor Dr. Philip Haellmigk ,LL.M., is the head of boutique law firm HAELLMIGK Lawyers in Munich, Germany, specializing in international trade, export controls, sanctions and compliance (www.haellmigk.com). Philip is qualified both as a German attorney and as a solicitor in England & Wales. Further, he holds law degrees from the University of Montpellier (France), a PhD from the University of Osnabrueck (Germany) and a LL.M. from Edinburgh Law School (Scotland). Philip is also a Professor of Law at the FOM University of Munich (Germany). Philip is fluent in English, French and German. He also speaks Spanish and Italian and has a basic knowledge of Mandarin. Philip is a frequent contributor to legal and business publications and regularly speaks at national and international conferences.

ABSTRACT

Since the Trump election, the subject of extra-territorial application of national law – in particular U.S. law – has received considerable attention. This is so because the U.S. administration increasingly uses this legal tool to enforce its foreign policy interests. A legal area with a particularly strong reach of extra-territoriality is U.S. export controls as this allows the U.S. to control foreign states' business. A very recent and vivid example is the Huawei trade ban by the U.S. The purpose of this article is to show the (harsh) legal and economic effects, which the extra-territorial application of U.S. export-related laws have on international trade.

The article will focus on the approach taken by the U.S. to impose its export controls outside the U.S. It will analyze the legal framework of extra-territorial U.S. export controls and explore to which extent the U.S. laws apply to foreign business, i.e., business outside the U.S. The article will define the cases in which foreign companies are subject to U.S. export controls and therefore must comply with U.S. regulations. It will show that the applicability of U.S. export controls to foreign companies and their business is considerably broad. It rigorously controls the destiny of U.S. origin products and components once they have been exported from U.S. territory and also regulates the worldwide export of products that have been manufactured by using

U.S. technology. In addition, U.S. export controls impose economic sanctions on countries (e.g., Iran) or companies (e.g., Huawei) and prohibit foreign companies from doing business with these sanctioned parties.

Understanding U.S. export controls and its extra-territorial reach are a challenge for foreign companies. It is a rather complex legal system that requires deeper knowledge of the underlying concept. However, foreign companies are well advised to comply with U.S. export controls, as the penalties for violations can be severe, including millions of dollars in fines and even imprisonment. In addition, the U.S. may blacklist foreign companies with the effect that business with the U.S. or elsewhere is no longer possible. Therefore, understanding U.S. export controls and its extra-territorial reach is vital to foreign companies.

TABLE OF CONTENTS

I. INTRODUCTION

At least since the U.S. authorities placed the Chinese company Huawei and its foreign subsidiaries on the blacklist in 2019 and subjected them to trade sanctions (the most recent restrictions against Huawei were implemented in August 2020), the issue of U.S. export controls & U.S. sanctions has once again moved to the forefront of attention for European businesses.

The reason why not only U.S. companies, but also European companies have to comply with U.S. export controls, is as follows: U.S. export controls have worldwide validity. That means that the U.S.A. demand that those companies trading outside the territory of the U.S. also comply with their export control regulations.

If companies fail to comply with U.S. export control regulations, then they face heavy fines and/or risk being placed on a U.S. trade blacklist. This was for example the case in the years 2014/15, when the French bank BNP Paribas and the German bank Commerzbank AG were ordered to pay about 9 and 1.5 billion USD in fines, respectively. In 2018, the Chinese telecom company ZTE was fined 1 billion USD and placed on a blacklist.

Against this background, it is essential for companies to be familiar with the basics of extra-territorial application of U.S. export controls and to integrate them into their compliance procedures.

The present contribution therefore provides a consolidated overview of the concept of U.S. export controls, explains the content and scope of its extra-territoriality and sets out the conditions under which U.S. export controls also apply to the trading activities of European companies.

II. THE CONCEPT OF GENERAL U.S. EXPORT CONTROLS

General U.S. export controls of cross-border trade outside the U.S.A. apply in two situations:

- the item to be exported is a U.S. item (criterion 1).
- a U.S. person is involved in the cross-border trade (criterion 2).[1]

A. Criterion 1: The Item to Be Exported Is a U.S. Item

There are three constellations in which the item qualifies as a U.S.-made item according to the understanding of U.S. export controls:

1. Constellation 1: The Item to Be Exported Has a U.S. Origin

An item is of U.S. origin if it was produced in the U.S.. Therefore, the relevant criterion is the place of

[1] Occasionally, other criteria are mentioned such as “US territory” or “U.S. dollar transactions”. This article, however, deals with U.S. export controls on foreign business outside the U.S.A., thus it is not concerned with business within, or from, the U.S. The processing of U.S. dollar transactions outside the U.S. always takes place in conjunction with commercial banks in the U.S. resulting in a U.S. person (U.S. bank) being involved in the foreign business. Therefore, this constellation is already covered by criterion 2.

production, respectively.[2] As regards the classification of an item as a U.S. item, it is thus irrelevant whether it has transited the U.S. or whether it was stored there. Furthermore, an item that was originally made abroad, but enhanced, reconditioned, assembled, or improved in its functionality in the U.S.A. is also classified as a U.S. item according to the practice of the U.S. authorities.[3]

If an item was produced in the U.S., then the U.S. origin of this item, as a general rule, remains unchanged. Therefore, an item produced in the U.S. does not lose its character as a U.S.-origin item even if it has been shipped to or transited through several countries after its manufacture in the U.S. Even when the item is repeatedly exported outside the U.S. it is and remains a U.S.-origin item.

However, an exception from this principle applies when the U.S.-made item is transformed into another item outside the United States. The new foreign-made item basically supersedes the original U.S.-made item.[4]

2. Constellation 2: The Item to Be Exported Is Made Outside the United States, But Contains U.S.-Origin Content

An item made outside the U.S. that contains U.S.-origin content is subject to U.S. export controls. However, this applies only if the U.S.-origin controlled content equals or exceeds a specified percentage value of foreign-made content (so-called de minimis rule).[5] The percentage value is 25%.

However, for deliveries to countries that are accused by the U.S. of supporting terrorism (Cuba, Iran, North Korea, Syria, Sudan), the allowed percentage value is merely 10%.

However, when applying the de minimis rule, the following aspects must be observed:

First of all, it must be noted that the de minimis rule must not be applied to all foreign-made items incorporating U.S.-origin content. For example, certain foreign-produced military commodities, peak performance computers or encryption technology are excluded from the rule. In these cases, the item is subject to U.S. export controls even if the value of the U.S. content incorporated in the foreign-produced item is minimal.[6] However, the de minimis rule can be used for the vast majority of foreign-made items incorporating U.S. content.

However, when calculating the percentage value, U.S. export controls do not require that all U.S.

[2] Cf. § 734.3(a)(2) Export Administration Regulations (EAR). From time to time, some authors comment that if the focus is on the question of the item's place of production, one fails to recognize that U.S. export controls also apply to items located in the U.S.A., i.e. the controls apply regardless of whether the items were produced there or not. This allegation may be true, but misses the point. In so far as exports from the U.S.A. are concerned, U.S. export controls, of course, also apply to the export of items located in the U.S.A. The term "U.S. item" then also refers to items that are located in the U.S.A. but have not been produced there. The present case, however, deals with the export of U.S. items outside the U.S.A., i.e., with so-called reexports. With regard to reexports, the term "U.S. item" is defined slightly different and refers to an item that has been produced in the U.S.

[3] Cf. Bureau of Industry and Security (BIS), *Complete list of Key terms used in the De minimis/Direct Product Decision Tool* (*as modified on 11 April 2018)*, https://www.bis.doc.gov/wrappers/ddpr/ddpr_interactive_tool_files/docs/Key%20terms%20used%20in%20Direct%20Product%20and%20De%20Minimis.pdf (accessed September 4, 2020).

[4] See for example Sec. 560.205 (b) (1) of the Iranian Transactions and Sanctions Regulations.

[5] § 734.3(a)(3)(ii) EAR. The *de minimis* rule also applies to foreign-made software and technology with incorporated (or commingled with) U.S.-origin controlled software and technology; cf. § 734.4(c), § 734.4(d) EAR.

[6] § 734.4(a)EAR.

contents incorporated in the foreign-made item be taken into account.

The most relevant exceptions include:

U.S.-origin content that is not classified under any Export Control Classification Number (ECCN) listed on the American dual-use list (i.e. Commerce Control List) can be disregarded when calculating the de minimis value. This applies to all U.S. contents that are designated as EAR99.[7]

However, even if the U.S. content is classified under an ECCN, this does not necessarily mean that it must be taken into account when calculating the de minimis value. This only applies if – assuming that the U.S.-origin content would be delivered separately – the ECCN for the country to which the U.S. content is to be shipped actually requires an export license. U.S. export controls refers to this as controlled U.S.-origin content. According to the concept of U.S. export controls, a U.S. content or U.S. item is not considered as controlled (subject to license) when it has an ECCN, but instead when the control reason stated in the respective ECCN, i.e. the reason why the item is listed on the Commerce Control List, also applies to the specific country of destination.[8]

There is even an exception to the principle that controlled U.S. content must be included in the de minimis calculation, namely, when certain control reasons apply and when it is possible to use a general license (license exception) for the specific country of destination. If, for example, the U.S. content has an ECCN because of "national security" control reasons only and the general license "GBS – Country to Group B Shipments" can be used, then it can be disregarded when calculating the value of the U.S. content in the foreign-produced item.[9]

3. Constellation 3: The Item to Be Exported Is Produced Outside the United States, But Is Based on U.S. Technology or U.S. Software

If the foreign-produced item uses U.S. technology, i.e. is directly produced by the use of said technology, then general U.S. export controls generally consider this to be a U.S.-origin item as well. The same applies if the foreign-produced item is the direct product of a plant located outside the U.S.

---

[7] Cf. BIS, *De minimis Rules and Guidance, § 734.4 and Supplement No. 2 to part 734 of the EAR (as modified on 5 November 2019)*, https://www.bis.doc.gov/index.php/documents/pdfs/1382-de-minimis-guidance/file (accessed September 4, 2020). However, in case of certain (embargoed) countries, the EAR99 content must be taken into account as well; cf. in this regard Philip Haellmigk, *Das Konzept der US-Re-Exportkontrolle – Eine systematische Erläuterung im Lichte des aktuellen US-Iran*-Embargos, 3 CORPORATE COMPLIANCE ZEITSCHRIFT, 135, 138 (2019); see also III.A.1 below.

[8] What matters in this respect are the reasons as to why the item was included on the Commerce Control List (reasons for control). For each country, a list of countries sets out whether the respective reason for control applies (Commerce Country Chart, cf. Supplement 1 to Part 738 EAR). Only a combination of the reason for control and the country of destination thus reveals whether the export of the item requires a license; for detailed information see Philip Haellmigk, *Das Konzept der US-Re-Exportkontrolle – Eine systematische Erläuterung im Lichte des aktuellen US-Iran*-Embargos, 3 CORPORATE COMPLIANCE ZEITSCHRIFT, 135, 137 (2019); Gabriele Burkert-Basler, *Fallstricke in der Operative: Reexportbeschränkungen der Export Administration Regulations*, 9 US-EXPORTBESTIMMUNGEN, 151, 151 (2019); Philip Haellmigk, *Die US-Re-Exportkontrolle: Konfusion oder Konzeption?*, 2 AW-PRAX – AUßENWIRTSCHAFTLICHE PRAXIS, 57, 58 (2019).

[9] Cf. § 740.4 EAR; cf. Supplement 2 to Part 734 – Guidelines for *de minimis* Rules, (1) (a); see also BIS, *De minimis Rules and Guidance, § 734.4 and Supplement No. 2 to part 734 of the EAR (as modified on 5 November 2019)*, https://www.bis.doc.gov/index.php/documents/pdfs/1382-de-minimis-guidance/file (accessed September 4, 2020); Philip Haellmigk, *Das Konzept der US-Re-Exportkontrolle – Eine systematische Erläuterung im Lichte des aktuellen US-Iran*-Embargos, 3 CORPORATE COMPLIANCE ZEITSCHRIFT, 135, 137 (2019); regarding the content and the conditions for using the various license exceptions cf. Philip Haellmigk, *Die License Exceptions in der US-Exportkontrolle*, 2 AW-PRAX – AUßENWIRTSCHAFTLICHE PRAXIS, 60, 60 et seq. (2020).

that was established using U.S. technology.[10]

However, the qualification of such a foreign-produced item as a U.S.-origin item does not apply without exception, but instead is subject to restrictions. It essentially depends on whether the item is to be shipped to certain critical countries and on for what control reasons the U.S. technology or U.S. software was classified under the relevant ECCN.[11]

B. Criterion 2: A U.S. Person Is Involved in The Cross-Border Trade

General U.S. export controls define a U.S. person as any

- natural person having U.S. citizenship including Green Card holders, regardless of their place of residence;
- natural persons permanently residing in the U.S., regardless of their nationality;
- a company incorporated under the laws of the U.S. including its dependent branch offices abroad.[12]

Vice versa, it follows that the following companies are not U.S. persons:

- A company incorporated under European laws;
- A company incorporated under European laws, even if it is the subsidiary of a U.S. company.

According to the above definition, general U.S. export controls only apply to those companies that were incorporated under U.S. laws. The relationship of a subsidiary of a U.S. company to the U.S. resulting from its U.S. group affiliation does not matter in this case.[13]

Thus, there is only one exception to the principle that companies incorporated under foreign laws are not U.S. persons and, therefore, do not have to comply with general U.S. export controls. This is the case when a U.S. employee holds a senior position (e.g., management) directly relating to the company's export transactions. Due to this employee's U.S. citizenship, the company basically becomes a U.S. person and is thus subject to general U.S. export controls.[14]

[10] § 734.3(a)(4); § 736.2(b)(3) EAR.

[11] Cf. BIS, *General Prohibition No. 3: Direct Product Rule - § 736.2(b)(3) of the EAR*, https://www.bis.doc.gov/index.php/licensing/reexports-and-offshore-transactions/direct-public-guidelines (accessed September 4, 2020). For specific sensitive items, special provisions apply; see for example § 736.2(b)(3)(iii) EAR. Regarding reexports to Huawei, the Foreign Direct Product rule has been modified to further restrict Huawei's access to sensitive U.S. technology and U.S. software, cf. Supplement 4 to Part 744 EAR – Entity List, footnote 1, see IV.B.1. below.

[12] Part 772 of the EAR – Definition of Terms: U. S. person.

[13] ERIC HIRSCHHORN, THE EXPORT CONTROL AND EMBARGO HANDBOOK, 199 (2nd ed., 2005); ED KRAULAND/PETER JEYDEL, Iran: sanctions minefield for non-U.S. companies, 52 WORLDECR – THE JOURNAL of EXPORT CONTROLS AND SANCTIONS 16, 16 (2016).

However, the U.S. group affiliation does play a role if shipments to embargoed countries are concerned, see below under III.A.2.

[14] In such a case, the company can lay down in the form of what is called a recusal policy that the U.S. person is debarred from carrying out export transactions ("walled off from export-related business"), so that the company is not considered as a U.S. person; cf. Office of Foreign Assets Control (OFAC), Frequently Asked Questions Relating to the Lifting of Certain U. S. Sanctions Under the Joint Comprehensive Plan of Action (JCPOA) on Implementation Day, last updated on December 15, 2015, C.16, https://home.treasury.gov/system/files/126/jcpoa_faqs.pdf (accessed September 4, 2020).

III. THE CONCEPT OF SPECIAL U.S. EMBARGO LAWS

From a systemic perspective, special U.S. embargo laws tighten the general U.S. export controls by extending the existing rules of general U.S. export controls or by establishing additional rules.

General U.S. export controls are tightened in two ways:

- Approach 1: Tightening the general criteria for U.S. item and U.S. person
- Approach 2: Introduction of a criterion: secondary sanctions.

A. Approach 1: Tightening Criteria U.S. Item and U.S. Person

Special U.S. embargo laws extend the existing criteria for general U.S. export controls, i.e. the criteria for U.S. item and U.S. person.

1. Tightening Criterion U.S. Item

First of all, the principle, that U.S. content classified under EAR99 is not included in the de minimis calculation, no longer applies. In case of specific embargoed countries, U.S. content classified under EAR99 must also be included in the de minimis calculation.[15]

In addition, the principle that the maximum admissible percentage value of U.S. content be valued at 25% or less is removed. For deliveries to certain countries embargoed by the U.S., the U.S. content in a foreign-made product must be valued at 10% or less. The U.S. embargo against Iran includes the extension of this criterion, for example. In this case, the U.S. content must be valued at less than 10%. Otherwise, it is a U.S.-origin item.[16]

2. Tightening Criterion U.S. Person

The principle that only businesses incorporated under U.S. laws are U.S. persons no longer applies. From now on, foreign subsidiaries of a U.S. parent company are treated as U.S. persons, too.[17]

The U.S. embargo against Iran, for instances, includes an extension of this criterion. Foreign companies belonging to a U.S. group are treated as U.S. persons. Consequently, they must observe the same trade restrictions on Iran as apply to their U.S. parent company as the U.S. person.[18]

---

[15] For deliveries to Cuba cf. § 746.2 (a) EAR; for deliveries to North Korea cf. § 746.4 (a) EAR; for deliveries to Crimea cf. § 746.6 EAR; see also Philip Haellmigk, *Die US-Re-Exportkontrolle: Konfusion oder Konzeption?*, 2 AW-PRAX – AUßENWIRTSCHAFTLICHE PRAXIS, 57, 59 (2019).

[16] Further examples of this include deliveries to or Cuba North Korea, Syria, Sudan, cf. § 734.4 (c), (d) EAR in conjunction with Country Group E:1, E:2 of Supplement No. 1 to Part 740 EAR.

[17] The treatment of U.S. foreign subsidiaries as equivalent to U.S. persons does not only apply if the U.S. company holds 50% or more of the shares, but also if it exercises a comparable controlling influence on the activity of the non-U.S. company; cf. in more detail Philip Haellmigk, *Das aktuelle US-Iran-Embargo und seine Bedeutung für die deutsche Exportwirtschaft: Das US-Sanktionsregime der Primary und Secondary Sanctions*, 1 CORPORATE COMPLIANCE ZEITSCHRIFT, 33, 34 (2018); Philip Haellmigk, *Das Konzept der US-Re-Exportkontrolle – Eine systematische Erläuterung im Lichte des aktuellen US-Iran-Embargos*, 3 CORPORATE COMPLIANCE ZEITSCHRIFT, 135, 138 (2019).

[18] ED KRAULAND/PETER JEYDEL, *Iran: sanctions minefield for non-U.S. companies*, 52 WORLDECR – THE JOURNAL of EXPORT CONTROLS AND SANCTIONS 16, 16 et seq. (2016); Philip Haellmigk, *Das aktuelle US-Iran-Embargo und seine Bedeutung für die deutsche Exportwirtschaft: Das US-Sanktionsregime der Primary und Secondary Sanctions,* 1 CORPORATE COMPLIANCE ZEITSCHRIFT, 33, 34 (2018).

B. Approach 2: Introduction of A New Criterion: Secondary Sanctions

In addition to the first approach of tightening up, i.e. the extension of the criteria for general U.S. export controls, U.S. embargo laws introduce a new criterion.
It sets forth that non-U.S. companies who neither export U.S. items nor qualify as a U.S. person within the meaning of general U.S. export controls are also subject to U.S. export controls. This new rule therefore applies to all non-U.S. companies.

Depending on the content of the U.S. embargo concerned, all non-U.S. companies worldwide are therefore prohibited from shipping specific products to a sanctioned country or to supply specific industries or companies in this country. The regulatory framework, which is using trade bans to target non-U.S. companies that neither export U.S. items nor are U.S. persons within the meaning of general U.S. export controls, is called secondary sanctions.[19]

The U.S. embargo against Iran, for example, includes secondary sanctions. Iran is, among others, subject to trade bans concerning, i.a., the following products, industries, and companies:

- the Iranian metal sector;
- the Iranian mining sector;
- the Iranian textiles sector;
- the Iranian automotive industry;
- the Iranian marine and shipbuilding sector;
- the Iranian oil industry;
- the Iranian construction sector;
- the Iranian energy sector
- the Iranian textile sector.

IV. THE U.S. SANCTIONS LISTS

A. The Concept of U.S. Sanctions Lists

Like the EU, the U.S also maintains numerous lists, which include natural persons, companies, and entities (collectively referred to as “companies”) that are subject to U.S. trade sanctions.[20]

The reasons as to why the U.S. draws up sanctions lists and puts a company on a sanctions list are numerous. The U.S. is, among others, interested in fighting international terrorism and drug trafficking,[21] in preventing the spread of weapons of mass destruction, and in other activities that pose

[19] For detailed information on the concept and content of secondary sanctions see Philip Haellmigk, *Das aktuelle US-Iran-Embargo und seine Bedeutung für die deutsche Exportwirtschaft: Das US-Sanktionsregime der Primary und Secondary Sanctions,* 1 CORPORATE COMPLIANCE ZEITSCHRIFT, 33, 36 et seq. (2018); Philip Haellmigk, *Das Konzept der US-Re-Exportkontrolle – Eine systematische Erläuterung im Lichte des aktuellen US-Iran-Embargos,* 3 CORPORATE COMPLIANCE ZEITSCHRIFT, 135, 138 (2019); see also Jeffrey A. Meyer, *Second Thoughts on Secondary Sanctions*, 1 U. Pa. J. Int'l L., 905, 905 et seq. (2009).

[20] Cf. in this regard Philip Haellmigk, *Die US-Sanktionslisten und ihre Bedeutung für europäische Unternehmen – Eine systematische Darstellung zu ihrem Inhalt, Umfang und ihrer Reichweite*, 3 CORPORATE COMPLIANCE ZEITSCHRIFT, 147, 147 et seq. (2020).

[21] Specially Designated Nationals and Blocked Persons List.

a threat to their national security.[22] The reason why a company is listed on a U.S. sanctions list can also be down to the fact that it has violated U.S. export controls.[23] Moreover, if there is no reliable information on the company, it will be classified as untrustworthy.[24]

Different U.S. authorities such as the Bureau of Industry and Security (BIS), the Office of Foreign Assets Control (OFAC), or the Directorate of Defense Trade Controls (DDTC) administer the U.S. sanctions lists.

These U.S. sanctions lists include:

- The Entity List
- The Denied Persons List (DPL)
- The Unverified List[25]
- The List of Administratively Debarred Parties
- The List of Statutorily Debarred Parties[26]
- Specially Designated Nationals and Blocked Persons List (SDN List)[27]
- The Foreign Sanctions Evaders List
- The Sectoral Sanctions Identifications List
- The Non-SDN Palestinian Legislative Council List
- The List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions (CAPTA List)
- The Non-SDN Iranian Sanctions Act (NS-ISA) List.[28]

Further, the extra-territorial claim of the U.S. sanctions lists is based on the same criteria with which general U.S. export control laws and special U.S. embargo laws control foreign business outside the U.S. territory (U.S. item, U.S. person, and secondary sanctions).

Therefore, the U.S. sanctions lists can be divided into three categories.

- Category 1: The U.S. sanctions list concerns a U.S. item
- Category 2: The U.S. sanctions list concerns a U.S. person
- Category 3: The U.S. sanctions list concerns a person or company against whom a worldwide embargo has been imposed (secondary sanctions).

[22] Cf. the Entity List.

[23] See the Denied Persons List.

[24] Cf. the Unverified List.

[25] Responsibility for the Entity List, the Denied Persons List, and the Unverified List lies with the BIS; they are summarized under the term "List of Parties of Concern"; cf. the BIS's homepage: https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern (accessed September 4, 2020).

[26] The List of Administratively and the List of Statutorily Debarred Parties are administered by the DDTC; see the DDTC's homepage: https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=c22d1833dbb8d300d0a370131f9619f0 (accessed September 4, 2020).

[27] The SDN List also includes the List of Persons Identified as Blocked Solely Pursuant to Executive Order 13599 ("the 13599 List").

[28] Responsible for all other sanctions lists is the OFAC; cf. OFAC's homepage: https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx (accessed September 4, 2020). The starting point for the OFAC's sanctions lists are what are called sanctions programs (i.e., legal acts), on the basis of which the U.S. sanctions lists and the list of companies are drawn up. Contrary to widespread opinion, a separate Non-Proliferation List (which is identified as such) does not exist. Instead, the "Non-Proliferation" sanctions program was used as a basis to identify companies involved in proliferation that were then listed on the SDN List. The various SDN entries refer to the respective sanctions program. Thus, an SDN List entry made on the basis of the sanctions program "Non-Proliferation Sanctions" contains the information "NPMWD" (Weapons of Mass Destruction Proliferators Sanctions Regulations); an entry on the SDN List based on the sanctions program "Counter Terrorism Sanctions" includes for example the information "FTO" (Foreign Terrorist Organization Sanctions Regulations") or "SDGT" (Global Terrorist Sanctions Regulations).

B. The Content & Scope of The Various U.S. Sanctions Lists

1. The Entity List

The BIS's Entity List includes companies that, from the U.S. point of view, threaten their national security or foreign policy interests.[29] It (only) applies to any trade with U.S. items by the listed companies.[30] The Entity List therefore belongs to the first category of U.S. the sanctions lists.

The (re)export of U.S. items requires a license from the BIS, and the Entity List already provides some information as to the chances of success of a license application (case-by-case review, presumption of approval, presumption of denial).[31]

2. The Denied Persons List

The BIS's Denied Person List designates companies against which a denial order has been issued due to violations of U.S. export controls.[32] This denial order deprives the companies on the list of the right to trade with U.S. items. At the same time, third parties are prohibited from trading with companies listed on this list in so far as it involves U.S. items.[33] This U.S. sanctions list therefore belongs to the first category of U.S. the sanctions lists.

The respective denial order on the company sets out the scope of the prohibition to trade with U.S. items. The BIS regularly issues a standard denial order that includes a comprehensive trade ban.[34] The denial order can be issued for an unlimited period or for only a limited period of time (temporary denial order), whereas this period may be as long as 50 years.

3. The Unverified List

The BIS's Unverified List includes companies whose (real) existence is not verifiable so that special care must be taken when dealing with companies on this list (red flag). It applies to the trade with U.S. items.[35] Hence, this U.S. sanctions list likewise belongs to the first category of the U.S. sanctions lists.

The unverified list generally does not contain any trade restrictions. Prior to the delivery, the exporter merely needs to obtain what is known as an unverified list (UVL) statement signed by the customer which, among others, includes information regarding the end use and an agreement to consent to

[29] Supplement 4 to Part 744 of the EAR.

[30] The Entity List indicates, for each company listed, whether the entry applies to all or only certain U.S. items. Generally, all U.S. items are listed, thus also EAR99 items. Regarding Huawei, BIS has amended the Foreign-Made Direct Product rule (see II.A.3. above) to further restrict Huawei's access to sensitive U.S. technology and U.S. software.

[31] Cf. § 744.16 EAR. Sometimes, the chances of success are generically stated for all U.S. items; sometimes, the evaluation is made with respect to individual U.S. items.

[32] Cf. https://www.bis.doc.gov/index.php/the-denied-persons-list (accessed September 4, 2020).

[33] Cf. Philip Haellmigk, *Bedeutung der U.S. Denied Persons List für deutsch-europäische Unternehmen*, 7/8 US-EXPORTBESTIMMUNGEN, 102, 103 (2018).

[34] However, the standard denial order does not prohibit any trade with foreign-produced items that are the direct product of U.S.-origin technology (for more on this type of item see II.A.3. above, cf. Philip Haellmigk, *Bedeutung der U.S. Denied Persons List für deutsch-europäische Unternehmen*, 7/8 US-EXPORTBESTIMMUNGEN, 102, 104 (2018).

[35] Supplement No. 6 to Part 744 of the EAR.

post-shipment controls.[36]

4. The List of Administratively / Statutorily Debarred Parties (Debarment List)

The DDTC's debarment list, which is divided into the List of Administratively Debarred Parties and the List of Statutorily Debarred Parties, lists companies that have violated U.S. arms export controls. They are debarred from purchasing U.S. military items, whereas the period of debarment is usually three years.[37]

As a result, the companies listed on the debarment list cannot participate in the trade with U.S. military items.[38] Therefore, these U.S. sanctions lists also belong to the first category of U.S. sanctions lists.

5. The Foreign Sanctions Evaders List

The OFAC's Foreign Sanctions Evaders List includes companies that have violated U.S. sanctions against Iran or Syria (pursuant to Executive Order 13608) or were implicated in business with persons who are subject to U.S. sanctions.

With respect to these companies, a comprehensive trade ban applies.[39] It is aimed at U.S. persons.[40] This U.S. sanctions list therefore belongs to the second category of U.S. sanctions lists.

6. The Sectoral Sanctions Identifications List

The OFAC's Sectoral Sanctions Identifications List cites Russian companies (such as banks and companies operating in oil-producing and oil-exploring industries) with whom certain trading activities are prohibited. The individual trade restrictions are provided in Directives 1, 2, 3 and 4 and, among others, contain prohibitions relating to credit and finance operations as well as to the delivery of items for oil production and exploration.[41]

These trade bans are aimed at U.S. persons.[42] Therefore, this U.S. sanctions list also belongs to the second category of the U.S. sanctions lists.

7. The Non-SDN Palestinian Legislative Council List

The OFAC's Non-SDN Palestinian Legislative Council List summarizes those persons who were elected to the Palestinian Legislative Council as representatives of a terrorist organization.

---

[36] § 744.15(b) EAR.

[37] § 127.7 ITAR.

[38] Hence, the trade ban does not cover civilian or dual-use items; cf. also Matthias Merz, *Compliance im Außenwirtschaftsrecht, in* Corporate Compliance no. 77 et seq. (*Christoph E. Hauschka et al. eds.,* 3rd ed. 2016).

[39] The trade ban thus also applies to business within the U.S.A., cf. the definition of U.S. persons under II.B.

[40] Cf. https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_iran.aspx#fse (accessed September 4, 2020).

[41] In certain cases, however, general licenses can be used, see https://www.treasury.gov/resource-center/sanctions/Programs/Pages/ukraine.aspx#directives (accessed September 4, 2020); in addition, it is possible to request an individual license from the OFAC for a commercial transaction which is, in principle, prohibited, although the chances of success of obtaining such a license are usually very low.

[42] The trade ban therefore also applies to business within the U.S., cf. the definition of U.S. persons under II.B.

Doing business with persons on this list is prohibited; the trade ban is aimed at U.S. persons.[43] Therefore, this U.S. sanctions list likewise belongs to the second category of U.S. sanctions lists.

8. The List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions

The OFAC's List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions lists financial institutions that are subject to restrictions or prohibitions relating to the opening of correspondent or payable-through accounts in the U.S.A.[44] Currently, there is only one foreign (Chinese) financial institution on the list.

These prohibitions are addressed to U.S. persons (U.S. financial institutions). Consequently, this U.S. sanctions list also belongs to the second category of U.S. sanctions lists.

9. The Non-SDN Iranian Sanctions Act List

The OFAC's Non-SDN Iranian Sanctions Act List identifies companies that are subject to various Iran-related trade bans.[45] The trade bans are addressed at U.S. persons (above all, U.S. financial institutions).

As a result, this U.S. sanctions list can likewise be attributed to the second category of U.S. sanctions lists.

10. The Specially Designated Nationals and Blocked Persons List

The OFAC's Specially Designated Nationals and Blocked Persons List is the largest U.S. sanctions list. On the one hand, it includes companies from countries that are subject to a U.S. embargo (country-specific). On the other hand, it lists companies that have connections with international terrorism or drug trafficking (not country-specific). With respect to these persons and companies on the list, a comprehensive trade ban applies.

With regard to the addressees of the trade bans, the Specially Designated Nationals and Blocked Persons List makes a distinction. Some trade bans are addressed to U.S. persons only, however, some are also addressed to non-U.S. persons.

Whether a trade ban also applies to non-U.S. persons can be recognized by the fact that the company's entry on the list contains the information "subject to secondary sanctions".[46] If this is the case, doing

[43] Provided that the members of the Palestinian Legislative Council have not been elected as representatives of a terrorist organization it is legal to do business with them, see General License No. 4, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/plc_gl4.pdf (accessed September 4, 2020).

[44] This U.S. sanctions list corresponds to the former List of Foreign Financial Institutions Subject to Part 561 (the Part 561 List).

[45] Cf. Section 6 Iran Sanctions Act.

[46] See for example the listing of Mines and Metals Engineering GmbH, a company subject to secondary sanctions: https://sanctionssearch.ofac.treas.gov/Details.aspx?id=2292; and the listing of Mamoun Darkazanli Import-Export Company, a company not subject to secondary sanctions: https://sanctionssearch.ofac.treas.gov/Details.aspx?id=343 (accessed September 4, 2020).

business with the company is prohibited, regardless of whether U.S. items are involved or not.[47]

If this entry is missing, the trade ban is restricted to U.S. persons.[48] As a result, this U.S. sanctions list belongs both to the second as well as to the third category of U.S. sanctions lists.

V. RESULTS

The question as to whether cross-border operations outside the U.S.A. are subject to U.S. export controls depends both on general U.S. export controls as well as on special U.S. embargo laws.

According to the rules established by general U.S. export controls, non-U.S. companies have to comply with U.S. export control law if the item to be exported is a U.S. item or if a U.S. person is involved in the cross-border trade.

An item is a U.S. item if the following conditions are met:

- The U.S. item has a U.S. origin.
- The item is produced outside the U.S. but has a U.S. content value of 25% or more.
- The item is made outside the U.S. but is produced directly with the use of U.S. technology.

A U.S. person is any

- natural person having U.S. citizenship including Green Card holders, regardless of their place of residence;
- natural persons permanently residing in the U.S., regardless of their nationality;
- a company incorporated under the laws of the U.S. including its dependent branch offices abroad.

Special U.S. embargo laws, such as for example the U.S. embargo against Iran, tighten these general rules. On the one hand, the content of the two criteria “U.S. item” and “U.S. person” is increased. Thus, items with a U.S. content value of 10% or more are classified as U.S. items. Also, non-U.S. companies that belong to a U.S. group are treated as a U.S. person.

Furthermore, a new criterion in the form of secondary sanctions is introduced. Secondary sanctions, as for example the U.S. embargo against Iran, include trade bans that target all non-U.S. companies, regardless of whether they export U.S. items or whether they are a U.S. person.

The U.S. sanctions lists reflect the approach taken by general U.S. export controls and specific U.S. embargo law. Therefore, the U.S. sanctions lists can be divided into three categories. Some U.S. sanctions lists (only) restrict the trade with U.S. items, but apply regardless of whether a U.S. company or a foreign company (re)exports the U.S. items. Other U.S. sanctions lists are expressly (only) addressed to U.S. persons. Finally, there are also sanctions lists that are expressly also aimed at

[47] Misleading Matthias Merz, *Compliance im Außenwirtschaftsrecht, in* Corporate Compliance no. 69 et seq. (*Christoph E. Hauschka et al. eds.,* 3rd ed. 2016).

[48] As regards companies listed on the SDN List that are not subject to secondary sanctions but listed due to their connections with terrorism, the BIS adds the following additional trade restrictions on non-U.S. persons: if a non-U.S. person wants to supply such a company with U.S. items, it must seek a license from the BIS, cf. § 744.12(a)(4) EAR, § 744.13(a)(4); § 744.14(a)(3) EAR.

non-U.S. persons, regardless of the nature of the items being traded.

The content of the trade restrictions of the various U.S. sanctions lists also varies. Sometimes, the trade requires an export license, sometimes the sanctions lists set out prohibitions that either apply to only certain transactions or to all transactions.

VI. CONCLUSIONS

Due to their extra-territorial application, European companies also have to comply with the requirements of U.S. export controls. Special caution is required when trading with companies from states that are subject to a U.S. trade embargo.

If they fail to observe U.S. export control regulations, they face severe fines by the U.S. authorities on the one hand. On the other, the companies are at risk of being placed on a blacklist by the U.S. authorities with the effect that U.S. companies will be prohibited from trading with them. The corresponding exclusion from the U.S. market can be life threatening to the company.

Therefore, European companies should ensure that their internal compliance procedures do not only comply with national and European export control regulations, but also reflect the requirements of U.S. export controls. It is vital to have an Internal Compliance Program for U.S. export controls.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

COMPLIANCE RISKS OF BLOCKCHAIN TECHNOLOGY, DECENTRALIZED CRYPTOCURRENCIES, AND STABLECOINS

Fabian Teichmann & Marie-Christin Falker

AUTHOR

Fabian M. Teichmann is an attorney-at-law and public notary in Switzerland. After earning an undergraduate degree in economics and finance (Bocconi University, Italy), he then earned graduate degrees in management (Harvard University, USA), accounting and finance, and law (University of St. Gallen, Switzerland). He also holds a PhD in law (University of Zurich, Switzerland), a doctoral degree in economics and social sciences (Kassel University, Germany), and an LL.M. (King's College, UK). Teichmann teaches courses on compliance, corruption, money laundering, and terrorism financing at various universities. He is the author of several books and over 100 scholarly articles.

Marie-Christin Falker is a graduate research associate at Teichmann International (Schweiz) AG. She possesses an undergraduate degree in English and American culture and business studies, focusing particularly on international management and marketing (Kassel University, Germany). She also studied at the University of Maryland, College Park (USA) as an undergraduate. Ms. Falker is currently pursuing a graduate degree in management, cultural studies and organizational theory at University of St. Gallen.

ABSTRACT

With the rise of digitalization, myriad new technologies are currently revolutionizing most, if not all, markets. One such technology that is receiving particular attention from businesses, private market participants, the financial sector, and governments alike is the blockchain. Despite its increasing popularity, most jurisdictions currently fail to adequately regulate it, meaning that businesses cannot exploit the full potential of blockchain technology and its various applications. This article explains how blockchains function and delineates their associated compliance risks. Here, particular attention will be paid to both decentralized cryptocurrencies and stablecoins. How decentralized cryptocurrencies could potentially be abused for money laundering, terrorism financing, and corruption purposes will be illustrated, and different legislation and international approaches to dealing with blockchain technology and cryptocurrencies will be highlighted. Lastly, the impact of

blockchain technology and its implications for actors in the digitalized economy will be discussed.

TABLE OF CONTENTS

I. INTRODUCTION

The blockchain is a phenomenon that attracts the attention of private actors, corporations, bankers, and governments alike. Naturally, it also attracts unwanted attention from certain criminals. Although its many unique offerings have the potential to revolutionize some, if not all, markets, the use of blockchain technology also raises a large number of compliance questions and concerns. Currently, most jurisdictions do not adequately regulate blockchain technology and its many areas of application, of which cryptocurrencies continue to be the most renowned. Regardless of the fact that the blockchain is a particularly relevant topic in the modern economic landscape, there is still much uncertainty associated with it.

This article clarifies some of the uncertainty surrounding blockchain technology by explaining its function in detail by using the Bitcoin blockchain as an example. What makes the blockchain so popular and how users can benefit from its use will be illustrated. At the same time, certain compliance risks associated with the blockchain, such as how decentralized cryptocurrencies may be abused for money laundering, terrorism financing, and corruption purposes, will be demonstrated by exploring some of the methods criminals could potentially use. The aim is to give compliance officers and prosecutors greater insight into how such criminals operate. The potential risks associated with stablecoins will also be discussed, especially with regard to the much-anticipated launch of Facebook's Libra. Lastly, legislation in different jurisdictions will be outlined and the possible implications thereof for different economic and private actors will be discussed.

II. WHAT IS THE BLOCKCHAIN?

The blockchain was created in 2008 to facilitate the launch of the first-ever digital currency: Bitcoin. The decentralized network[1] connects a multitude of computers referred to as "nodes." With regular, government-issued currencies (fiat), banks document all transactions on a central server in order to avoid double-spending. In contrast, Bitcoin is not governed by a central entity. Instead, blockchain technology facilitates so-called "peer-to-peer" transactions between individuals or businesses, meaning that they do not rely on the involvement of a trusted third party such as a financial intermediary.[2] The blockchain was created by the developer of Bitcoin, who operates under the alias Satoshi Nakamoto, in order to solve the issue of double-spending. This technological breakthrough revolutionized the market, as previously it had not been possible to create a digital currency.[3] Due to the lack of intermediaries, blockchain transactions are cheaper and faster than (international) bank transfers. They may be conducted without either restriction or incurring high transaction fees between any two locations in the world.[4]

[1] Salvatore Iacangelo, *Blockchain – Einordnung, Projekte und Chancen,* JUSLETTER 1, 1 (June 4, 2018), at 1.

[2] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf (last visited November 19, 2019).

[3] Blockgeeks, *Was ist eine Kryptowährung?,* https://blockgeeks.com/guides/de/was-ist-kryptowahrung/ (last visited November 19, 2019).

[4] Satoshi Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System,* https://bitcoin.org/bitcoin.pdf (last visited November 19, 2019).

Every node in the blockchain has a complete copy of the blockchain, and the blockchain is updated automatically as soon as a new block is added.[5] In this manner, the entirety of the blockchain irreversibly documents all transactions, which is why it is also referred to as a distributed ledger.[6] For this reason, the technology and its inherent characteristics engender trust. In contrast, users' trust in fiat is usually inspired by governmental regulations and official institutions such as central banks. Blockchain technology is considered to be highly secure, at least from the user's perspective, as it can hardly be manipulated.[7] In addition, the documentation of all transactions ensures transparency.

At the same time, however, most jurisdictions fail to regulate blockchain technology adequately. Although facilitating monetary transactions through cryptocurrencies is its most well-known application, blockchain technology offers the potential to be used in many other areas by enabling legal transfers of all kinds of tokens.[8] Tokens are entities of value on the blockchain that may represent claims or membership rights to finance companies, ownership rights to real assets, securities, and confidential documents such as birth certificates, among others.[9] Within the scope of digital currencies, tokens are referred to as (crypto) coins. Blockchain technology could further be used in international trading, investment, and more.

III. FUNCTIONING OF THE BLOCKCHAIN

At the outset, it must be stressed that there are multiple public and private blockchains, which may vary in their functioning. The following descriptions are based on the Bitcoin (public) blockchain, as it was the first one created. The blockchain is characterized by two inherent peculiarities: immutability and irrefutability.[10] The blockchain is a public database[11] consisting of individual blocks that are connected to one another chronologically. These blocks contain digital information about transactions. This information consists of the time, date, and amount transferred, as well as the addresses of peers and the so-called hash code, which functions as a unique identifier for the block. The user address is an array of numbers and letters to which other users may send tokens. Each user receives a private key and a public key. The private key is used to sign for transactions and access one's tokens; from the

[5] Luke Fortney, *Blockchain Explained,* https://www.investopedia.com/terms/b/blockchain.asp (last visited November 19, 2019).

[6] Jeanne L. Schroeder, *Bitcoin and the Uniform Commercial Code*, 458 CARDOZO LEGAL STUDIES RESEARCH PAPER 6 (August 22, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2649441 (last visited November 27, 2019).

[7] Luke Fortney, *Blockchain Explained,* https://www.investopedia.com/terms/b/blockchain.asp (last visited November 19, 2019).

[8] Government of Liechtenstein, Report and Application of the Government to the Parliament of the Principality of Liechtenstein Concerning the Creation of a Law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) and the Amendment of Other Laws, No. 54/2019, at 5.

[9] Government of Liechtenstein, Report and Application of the Government to the Parliament of the Principality of Liechtenstein Concerning the Creation of a Law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) and the Amendment of Other Laws, No. 54/2019, at 14.

[10] Rainer Böhme & Paulina Pesch, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, 8 DUD 473 (2017).

[11] Joachim Galileo Fasching, *Anwendungsbereiche und ausgewählte Rechtsfragen der Blockchain-Technologie* [Master's thesis] http://www.it-law.at/publikation/anwendungsbereiche-und-ausgewaehlte-rechtsfragen-der-blockchain-technologie/, at 3 (last visited November 19, 2019).

public key, the address is generated.[12] If the private key is lost or stolen, there is no way for the user to regain access to their tokens. There is also no central entity able to disable the key. Consequently, users must handle their keys with extreme caution. Millions of Bitcoins have already been lost because users have mixed up the numbers or letters when sending tokens to a Bitcoin address.[13]

The chronological addition of new blocks to the blockchain follows the "blockchain protocol." [14] Consensus protocols such as the blockchain protocol "ensure a common, unambiguous ordering of transactions and blocks"[15] while ensuring integrity and consistency across geographically distributed nodes. Before being added to the chain, every block is "hashed." The hash is a unique code that demarcates individual blocks. Every block receives both its own hash and the hash of the previously added block.[16] When hackers try to manipulate one specific transaction, the hash code of the block changes. However, the following block will continue to have the old hash. Thus, manipulations will be obvious. If the hackers decide to alter the following block so that the hashes match again, this block's hash will be altered, as well. Consequently, a chain reaction is triggered. Only when every following block is manipulated could hackers actually alter a transaction without being detected. However, this process would require immense and extremely costly computing power. In addition, they would need to solve the consensus model problem.[17] Thus, hacking the blockchain seems a rather unprofitable endeavor.

Once a transaction on the blockchain has been initiated, the tokens are collected in a common pool. The transaction must then be validated by a so-called "full weight node." Upon verification, the transaction is documented in a block and can no longer be altered.[18] All documented transactions can be viewed by everyone.[19] The verification of transactions and the addition of blocks to the blockchain are called "mining." So-called "lightweight nodes" ensure that this process is conducted correctly. Thus, they safeguard the integrity of the network.[20] New blocks are generated approximately every 10 minutes.[21] Mining is highly profitable because miners receive coins in exchange for their work. In order to prevent abuse, they must solve complex mathematical problems before they are approved to mine. These problems are called "consensus models," or in the case of Bitcoin, "proof of work." Answering

[12] Martin Hess & Stephanie Lienhard, *Übertragung von Vermögenswerten auf der Blockchain*, JUSLETTER 3, 1 (December 4, 2017).

[13] Jeff John Roberts & Nicolas Rapp, *Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says,* https://fortune.com/2017/11/25/lost-bitcoins/ (last visited November 19, 2019).

[14] Kariappa Bheemaiah, *Block Chain 2.0: The Renaissance of Money,* https://www.wired.com/insights/2015/01/block-chain-2-0/ (last visited November 19, 2019).

[15] Emmanuelle Ganne, Can Blockchain Revolutionize International Trade? 121 (2018).

[16] Michael Crosby et al., *BlockChain Technology – Beyond Bitcoin,* Sutardja Center for Entrepreneurship & Technology Technical Report 5 (2015), http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf (last visited November 19, 2019).

[17] Luke Fortney, *Blockchain Explained,* https://www.investopedia.com/terms/b/blockchain.asp (last visited November 19, 2019).

[18] Martin Hess & Patrick Spielmann, *Cryptocurrencies, Blockchain, Handelsplätze & Co. – Digitalisierte Werte und Schweizer Recht*, in Kapitalmarkt – Recht Und Transaktionen XII, 145 (Thomas U. Reutter & Thomas Werlen, eds., 2017).

[19] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System,* https://bitcoin.org/bitcoin.pdf (last visited November 19, 2019).

[20] Kai Schiller, *Blockchain Node – Lightweight und Full Nodes,* https://blockchainwelt.de/blockchain-node-lightweight-nodes-und-full-nodes-bitcoin-ethereum/ (last visited November 19, 2019).

[21] Jake Frankenfield, *51% Attack,* https://www.investopedia.com/terms/1/51-attack.asp (last visited November 19, 2019).

such problems requires expensive computer software. In addition, the probability of solving a proof-of-work problem is one in 5.8 trillion. The intention is to make hacking unprofitable.[22]

Evidently, mining is a full-time occupation that is difficult and requires significant expertise. However, established miners can generate high revenue and profit. Therefore, mining has become an industry that is dominated by multiple large firms. For instance, the Beijing "mining giant"[23] Canaan Creative has seen net profits of over US$17 million "on total revenues which approached US$400 million"[24] in 2018. In the crypto mining industry, the Peking mining cooperative Bitmain holds an approximately 80% share and generated over US$2.5 billion in revenue in 2017.[25] These numbers demonstrate why miners would enter the industry, even if doing so is difficult.

A. Compliance Risk: 51% Attack

The 51% attack refers to a hypothetical situation in which it would be possible to hack the (Bitcoin) blockchain. As previously outlined, hacking the blockchain would be difficult to achieve. In order to be able to effectively attack the blockchain, a group of miners would need to be able to control at least 51% of the network's computing power or mining hash rate.[26] In such an instance, the hackers could disrupt payments between some or all of the blockchain's users. In addition, they would be able to reverse transactions and double-spend coins.[27] Furthermore, they could interfere with the process of completing new blocks. In this way, the (profitable) mining of blocks could be monopolized. However, it is unlikely that a 51% attack would destroy the blockchain-based currency in question entirely, as the hackers would probably not be able to create new coins or alter old blocks that were created before the attack.[28]

In July 2014, the mining pool ghash.io exceeded 50% of Bitcoin's computing power; however, it voluntarily reduced its share to less than 40% to ensure that Bitcoin maintains its integrity. Two Ethereum-based blockchains, Krypton and Shift, were subject to 51% attacks in August 2016, and Bitcoin Gold suffered a 51% attack in May 2018. The hackers double-spent for days, which allowed them to steal over US$18 million in Bitcoin Gold. Another distributed ledger, Tangle, which is, however, distinct from the blockchain, could even be controlled via a 34% attack.[29]

---

[22] Luke Fortney, *Blockchain Explained,* https://www.investopedia.com/terms/b/blockchain.asp (last visited November 19, 2019).

[23] William Suberg, *Bitcoin Miner Canaan Creative's 2019 Revenue Nears $100M Ahead of IPO,* https://cointelegraph.com/news/bitcoin-miner-canaan-creatives-2019-revenue-nears-100m-ahead-of-ipo (last visited November 28, 2019).

[24] William Suberg, *Bitcoin Miner Canaan Creative's 2019 Revenue Nears $100M Ahead of IPO,* https://cointelegraph.com/news/bitcoin-miner-canaan-creatives-2019-revenue-nears-100m-ahead-of-ipo (last visited November 28, 2019).

[25] Rakesh Sharma, *Bitcoin's Biggest Mining Pool Operator Did More Than $2.5 Billion In Revenue Last Year,* https://www.investopedia.com/news/bitcoins-biggest-mining-pool-operator-did-more-25-billion-revenue-last-year/ (last visited November 28, 2019).

[26] Jake Frankenfield, *51% Attack,* https://www.investopedia.com/terms/1/51-attack.asp (last visited November 19, 2019).

[27] Jake Frankenfield, *51% Attack,* https://www.investopedia.com/terms/1/51-attack.asp (last visited November 19, 2019).

[28] Jake Frankenfield, *51% Attack,* https://www.investopedia.com/terms/1/51-attack.asp (last visited November 19, 2019).

[29] Jake Frankenfield, *51% Attack,* https://www.investopedia.com/terms/1/51-attack.asp (last visited November 19, 2019).

B. Transparency

One aspect of the blockchain that could increase its security is its transparency. As previously outlined, the high transparency of the blockchain is one of its most redeeming qualities. After all, blockchain technology could make multiple processes more efficient and economical, such as international trade (which is currently highly paper intensive and rather inefficient) and the accurate documentation of individual stops in a supply chain. Presently, these processes are comparatively opaque and expensive.[30]

IV. APPLICATIONS OF BLOCKCHAIN TECHNOLOGY: CRYPTOCURRENCIES

A. Decentralized Cryptocurrencies

Cryptocurrencies are virtual or digital money in the form of tokens or coins. The term "crypto" refers to the manner in which new tokens are generated, stored, and traded since these mechanisms are based on cryptography.[31] The field of cryptocurrencies is constantly expanding. However, Bitcoin continues to be the most well-known and influential cryptocurrency in terms of its user base, popularity, and market capitalization.[32]

Besides Bitcoin, other virtual currencies, such as Ethereum and Ripple, are becoming more popular, although they are used predominantly for enterprise solutions.[33] Most cryptocurrencies are designed to be "free from government manipulation and control."[34] Cryptocurrencies that are modeled after Bitcoin with the intent to improve upon it are called "altcoins."[35] While some altcoins might be easier to mine than Bitcoin, they require certain tradeoffs, such as lower liquidity (which increases risks) and less acceptance and value retention. Currently, there are more than 1,600 cryptocurrencies in existence.[36]

[30] SAP, *Blockchain – International Trade,* https://www.youtube.com/watch?v=-N_jAJyh8_E (last visited November 19, 2019).

[31] Prableen Bajpai, *The 10 Most Important Cryptocurrencies Other Than Bitcoin,* https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin (last visited November 19, 2019).

[32] Prableen Bajpai, *The 10 Most Important Cryptocurrencies Other Than Bitcoin,* https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin (last visited November 19, 2019).

[33] Prableen Bajpai, *The 10 Most Important Cryptocurrencies Other Than Bitcoin,* https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin (last visited November 19, 2019).

[34] Prableen Bajpai, *The 10 Most Important Cryptocurrencies Other Than Bitcoin,* https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin (last visited November 19, 2019).

[35] Prableen Bajpai, *The 10 Most Important Cryptocurrencies Other Than Bitcoin*, https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin (last visited November 19, 2019).

[36] Prableen Bajpai, *The 10 Most Important Cryptocurrencies Other Than Bitcoin,* https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin (last visited November 19, 2019).

1. Compliance Risks

a) Transparency

With regard to cryptocurrencies, the previously illustrated opportunities to ensure transparency usually do not apply. With Bitcoin, for instance, transactions are pseudonymous, not fully anonymous; however, they are not fully transparent, either. Users receive an address to which the coins are sent. Transactions made using this address can be seen by everyone due to the inevitable documentation that follows.[37] However, addresses usually cannot be traced back to their beneficial owners. This lack of know-your-customer (KYC) and the anti-money laundering (AML) regulations represent a serious compliance concern. Bitcoin partially solves this concern through its proof-of-work system that is supposed to increase user security. However, with regard to money laundering, terrorism financing, and corruption, this relative lack of transparency in crypto transactions offers opportunities for criminal activity to flourish.

b) Money Laundering

Compliance experts argue that due to strict AML and KYC guidelines in the financial sector, money launderers are increasingly relocating to less regulated sectors, such as jewelry and real estate.[38] In addition, law enforcement agencies and compliance officers around the world continue to voice their concerns about the ineffectiveness of AML efforts.[39] Currently, most jurisdictions do not sufficiently regulate blockchain technology,[40] which is why cryptocurrencies in particular are highly suitable for money laundering. As indicated above, they lack transparency and ensure high levels of anonymity.

The money laundering process consists of three steps: placement, layering, and integration.[41] Cryptocurrencies are suitable for the first two steps. During placement, the value carrier of the incriminated funds is changed, so they cannot immediately be traced back to the crime from which they originate. During the layering stage, anonymity and plausibility are created. Meanwhile, the origin of the incriminated funds is disguised.

In order to place their incriminated funds, money launderers may use part of them to purchase crypto coins. Cryptocurrencies can be purchased at crypto exchanges, broker exchanges, or automated teller machines (ATMs). Criminals without much expertise might prefer to employ crypto exchanges, as they are simple to use.[42] However, they usually require users to register and provide identification.

---

[37] Jean-Daniel Schmid & Alexander Schmid, Bitcoin – Eine Einführung in die Funktionsweise sowie eine Auslegeordnung und erste Analyse möglicher Rechtlicher Fragestellungen, JUSLETTER 12, 1 (June 4, 2012), at 12.

[38] FABIAN TEICHMANN, UMGEHUNGSMÖGLICHKEITEN DER GELDWÄSCHEREIPRÄVENTIONSMASSNAHMEN 25 (2016).

[39] Bruno S. Sergi & Fabian Teichmann, Compliance in Multinational Corporations – Business Risks in Bribery, Money Laundering, Terrorism Financing and Sanctions 31 (2018).

[40] The blockchain is only regulated in a handful of countries. See: Darya Yafimava, *Blockchain and the Law: Regulations Around the World*, https://openledger.info/insights/blockchain-law-regulations/ (last visited November 19, 2019).

[41] Bruno S. Sergi & Fabian Teichmann, Compliance in Multinational Corporations – Business Risks in Bribery, Money Laundering, Terrorism Financing and Sanctions 33 (2018).

[42] BitDegree, *Full Information on Where and How to Buy Cryptocurrency,* https://www.bitdegree.org/tutorials/how-to-buy-cryptocurrency/ (last visited November 20, 2019).

Broker exchanges, on the other hand, frequently charge high fees—especially for credit card payments. In addition, they sometimes enforce AML and KYC measures, including cooperating with local authorities. The third option, crypto ATMs, offers comparatively high levels of anonymity. These ATMs are becoming increasingly common worldwide.[43]

Consequently, from a money launderer's perspective, a crypto ATM would be the safest way to purchase crypto coins, especially since not all crypto ATMs require identification. Sometimes only a phone number is required. The launderer could use a disposable phone to receive the verification code from the ATM. The launderer would then enter the code into the ATM and deposit the cash; the case is then converted into cryptocurrency and sent to the launderer's wallet. If the launderer does not already have a wallet, the ATM will even create a new one for them.[44] The receipt issued by the machine can simply be disposed of, and with it, the transaction's paper trail ends. This method requires little effort and guarantees high anonymity—ATM locations can easily be found online (e.g., Coinatmradar.com).

Peer-to-peer exchanges are another option for launderers. Usually, users can register with them for free and providing identification is not mandatory. Peer reviews enhance security and there are frequently options to pay in cash. However, it might be difficult to find trustworthy sellers, and these exchanges are often difficult to use.[45] Alternatively, money launderers could attempt to find miners who would send them coins from different addresses in exchange for cash via the darknet.

To layer their funds, launderers may transfer crypto coins to different addresses that they own. At the same time, a variety of different crypto exchanges could be used. Thus, the cryptocurrency may be exchanged several times. Alternatively, they could use a software program called "Mixer," which divides their crypto assets and sends them to multiple addresses on the darknet, thereby preventing the individual transactions from being connected to one another. Thereafter, the funds are pooled again.

Finally, the crypto assets may either be exchanged back into fiat or kept as an investment. If the money launderer does not immediately need the funds, they could hold them as capital assets. For storage, a hardware (i.e., physical) wallet seems to be the safest option, as it leaves no digital trail and can be stored in a safe location. However, the money launderer must not lose the wallet or their assets would be lost as well. A physical wallet can be bought in a store with cash to prevent creating a paper trail. To further lower the risk of being identified, the money launderer could have a straw man purchase the wallet in cash on their behalf.

c) Terrorism Financing

Terrorist financiers may also use the methods outlined above to purchase cryptocurrency. Thereafter, the funds are simply transferred to the crypto address of a terrorist organization. To increase their anonymity, the person sending the funds could install a virtual private network (VPN) to make it seem

[43] Coin ATM Radar, *Bitcoin ATM Map,* https://coinatmradar.com/ (last visited November 15, 2019).

[44] BitDegree, *Full Information on Where and How to Buy Cryptocurrency,* https://www.bitdegree.org/tutorials/how-to-buy-cryptocurrency/ (last visited November 20, 2019).

[45] BitDegree, *Full Information on Where and How to Buy Cryptocurrency,* https://www.bitdegree.org/tutorials/how-to-buy-cryptocurrency/ (last visited November 20, 2019).

as though they are located in a different place to where they actually are. In the event of an investigation, they could claim to use the VPN for data protection purposes or to access programming that is not included on the domestic version of a given streaming service. Compared to using traditional financial institutions, sending cryptocurrency is a much safer option for terrorist financiers due to the anonymity it offers because not all crypto exchanges carry out KYC and AML procedures.

d) Corruption

Many multinational corporations reward employees based on their performance and incentivize high sales numbers. Consequently, employees might feel pressured to reach the targets set for them by their employers, even if they have to resort to illegal means such as bribery to do so.[46] At the same time, some business partners in countries with weak compliance regulations might even expect to be paid bribes.[47] When dealing with corrupt foreign officials, employees might feel as if they have no other option than to pay a bribe to secure a contract and receive a performance bonus. This type of corruption is referred to as Business to Government corruption and considered petty corruption, which refers to "everyday abuse of entrusted power by public officials […]".[48]

Employees who decide to bribe a corrupt foreign official, for example, could use cryptocurrencies for this purpose. Cryptocurrencies offer the advantage of making it difficult for the authorities to identify the beneficial owners behind the addresses. Therefore, the employee could utilize one of the previously outlined methods to purchase cryptocurrency and then transfer it to the corrupt official. Here, they may also employ anonymizing technology such as VPNs or even the darknet.

In the event that an employee refuses to pay a bribe to these business partners in order to comply with their company's guidelines, the other parties might instead choose to deal with competitors who are willing to pay bribes. As a result, the employee would be unable to meet their sales benchmarks and additionally lose out on their performance bonus. Therefore, it can be expected that many employees would be willing to take the risk. After all, the worst possible outcome for them would be that they lose their job. For the company, on the other hand, a corruption scandal could have disastrous consequences, including prison time for executive directors and unlimited fines.[49] The company could even have to declare bankruptcy, which would cause shareholders to lose their investment.

B. Stablecoins

Stablecoins represent a less volatile (in terms of value) digital currency than most decentralized cryptocurrencies (e.g., Bitcoin). The value of Bitcoin peaked in December 2017 at US$19,891.00 per Bitcoin. As of October 26, 2020, the Bitcoin price sits at roughly US$13,000 at a market cap of US$242.23 billion and a supply of 18.53 million coins.[50] The total number of Bitcoins created was set

[46] FABIAN TEICHMANN, ANTI-BRIBERY COMPLIANCE INCENTIVES 8 (2017).

[47] Peter Rodriguez et al., Government Corruption and the Entry Strategies of Multinationals, 30 AMR, 383 (2005).

[48] Transparency International, Petty corruption, https://www.transparency.org/en/corruptionary/petty-corruption# (last visited Oktober 26, 2020).

[49] ERM Initiative Faculty & Meredith Freeman, *Riskiness of Incentive Compensation Plans*, https://erm.ncsu.edu/library/article/riskiness-of-incentive-compensation-plans (last visited October 26, 2019).

[50] Coindesk, *Bitcoin (07/18/2010 to 10/26/2020),* https://www.coindesk.com/price/bitcoin (last visited November 19, 2019).

by Satoshi Nakamoto at 21 million coins.[51] The supply increases steadily in accordance with a predetermined schedule. This schedule remains unaffected by fluctuations in demand.[52]

Many private market participants and businesses are appalled by the immense fluctuations in value associated with decentralized cryptocurrencies. Stablecoins, on the other hand, were designed to maintain a stable value.[53] Stablecoins can be assigned to one of three categories: traditional collateral (asset backed, fiat backed, or both asset and fiat backed), crypto collateral (crypto asset backed or crypto asset and fiat backed), and algorithmic (backed by seigniorage [= the difference between the production cost and face value of money],[54] shares, fees, or a combination of the two). Traditional collateral stablecoins make up 31% of all stablecoins and are usually backed by one or multiple fiat currencies and/or gold. The most common type of stablecoin is crypto collateral. These currencies make up 52% of all stablecoins. Algorithmic stablecoins are the rarest kind, making up only 17% of all stablecoins. Currently, the most influential stablecoin is Tether, which was launched in 2014 and has a market value of US$2 billion.[55]

According to industry experts, the extremely highly sought-after applications of blockchain technology in the areas of payments, lending, and insurance require more stable digital currencies than Ethereum and Bitcoin.[56] As a result, user demand for stablecoins could increase in the near future, as they promise less volatile values. Garrick Hileman, who is head of research at the company Blockchain, argues that non-volatile cryptocurrencies could establish an "infrastructural layer" that would increase the number of cryptocurrency users on a global scale.[57] Currently, most stablecoin projects are based in and registered in Europe and the United States. This is relevant in terms of regulation.

Stablecoins are frequently used for trade with other cryptocurrencies. The more decentralized a stablecoin is, the less confident users usually are in its price stability.[58] Proponents of stablecoins argue that they offer individuals who do not have access to the banking sector or a stable national currency the opportunity to conduct monetary transfers.[59] In conjunction with their allegedly less volatile

[51] Ronald-Peter Stoeferle & Mark J. Valek, *Gold and the Turning of the Monetary Tides*, IN GOLD WE TRUST REPORT 243 (May 29, 2018), https://ingoldwetrust.report/reports-archive/in-gold-we-trust-2018/ (last visited October 26, 2020).

[52] Ronald-Peter Stoeferle & Mark J. Valek, *Gold in the Age of Eroding Trust*, IN GOLD WE TRUST REPORT 177 (May 28, 2019), https://ingoldwetrust.report/wp-content/uploads/2019/05/In-Gold-We-Trust-2019-Extended-Version-english.pdf. (last visited October 26, 2020).

[53] Mike Orcutt, *Stablecoins Will Help Cryptocurrencies Achieve World Domination – If They Actually Work,* https://www.technologyreview.com/s/612207/stablecoins-will-help-cryptocurrencies-achieve-world-domination-if-they-actually-work/ (last visited November 19, 2019).

[54] Christina Majaski, *Seignorage,* https://www.investopedia.com/terms/s/seigniorage.asp (last visited November 19, 2019).

[55] Blockchain, *2019 State of Stablecoins,* https://www.blockchain.com/research, at 7 (last visited November 19, 2019).

[56] Blockchain Team, *Shining Light on the State of Stablecoins,* https://blog.blockchain.com/2018/09/26/the-state-of-stablecoins/ (last visited November 19, 2019).

[57] Blockchain Team, *Shining Light on the State of Stablecoins,* https://blog.blockchain.com/2018/09/26/the-state-of-stablecoins/ (last visited November 19, 2019).

[58] Blockchain, *2019 State of Stablecoins,* https://www.blockchain.com/research, at 20, 27 (last visited November 19, 2019).

[59] Mike Orcutt, *Stablecoins Will Help Cryptocurrencies Achieve World Domination – If They Actually Work,* https://www.technologyreview.com/s/612207/stablecoins-will-help-cryptocurrencies-achieve-world-domination-if-they-actually-work/ (last visited November 19, 2019).

values, this aspect of stablecoins makes them attractive to users. At the same time, many types of stablecoins could be too difficult for inexperienced users to deal with. In addition, the lack of regulatory standards creates space for the myriad well-known compliance risks associated with cryptocurrencies to take hold. Ultimately, stablecoins give rise to many complicated legal questions.[60]

1. Compliance Risk: Libra

Due to the extensive discussions pertaining to Facebook's announced stablecoin, Libra, the compliance risks of stablecoins will be discussed here with a particular focus on Libra. Libra's internationally awaited launch had been scheduled for 2020[61], but due to a G7 draft, according to which stablecoins must not launch before they have been regulated as well as extensive criticism from central banks and government, the launch will likely be postponed until December 2022.[62]

Libra is governed by the Geneva-based Libra Association, which counts renowned corporations such as Coinbase, Uber, and Spotify as well as nonprofit organizations among its members.[63] The Libra Association defines its mission as follows: "The Libra Association's mission is to enable a global payment system and financial infrastructure that empowers billions of people", by fostering financial inclusion, reducing costs, and enabling new functionality.[64] According to its *White Paper*, the Libra Association aims to give people who do not have access to the financial system the opportunity to access financial services and favorable capital. To use Libra, users will simply require a phone and access to the internet. The Libra Association also argues that global, open, direct, and favorable monetary transactions will lead to an increase in global trade.[65]

Contrary to cryptocurrencies like Bitcoin, Libra was originally designed to be centralized while being powered by blockchain technology. The main difference would have been that all Libra nodes would have been under the control of the Libra Association instead of individual users. It had been argued that due to the fact that blockchain technology is more restricted with Libra, it is more of a digital currency than a cryptocurrency.[66] However, the Libra Association had claimed that '"Libra is indeed a cryptocurrency, though, and by virtue of that, it inherits several attractive properties of these new

[60] Mike Orcutt, *Stablecoins Will Help Cryptocurrencies Achieve World Domination – If They Actually Work,* https://www.technologyreview.com/s/612207/stablecoins-will-help-cryptocurrencies-achieve-world-domination-if-they-actually-work/ (last visited November 19, 2019).

[61] The Economist, *What is Libra?,* https://www.economist.com/the-economist-explains/2019/07/12/what-is-libra (last visited November 19, 2019).

[62] G7 Working Group on Stablecoins, *Investigating the impact of global stablecoins* (October 2019), https://www.bis.org/cpmi/publ/d187.pdf (last visited October 26, 2020); Ledgerinsights.com, *No Facebook Libra stablecoin launch before central banks explore digital currencies (CBDC)* (October 2020), https://www.ledgerinsights.com/no-facebook-libra-stablecoin-launch-before-central-banks-explore-digital-currencies-cbdc/ (last visited October 26, 2020).

[63] Libra.org, *Die Libra Association,* https://libra.org/de-DE/association/ (last visited November 19, 2019).

[64] Libra.org, *Libra White Paper,* https://libra.org/en-US/white-paper/?noredirect=1#the-libra-currency-and-reserve (last visited November 20, 2019).

[65] Libra.org, *Libra White Paper,* https://libra.org/de-DE/white-paper/#the-libra-currency-and-reserve (last visited November 20, 2019).

[66] Libra.org, *Libra White Paper,* https://libra.org/de-DE/white-paper/#the-libra-currency-and-reserve (last visited November 20, 2019).

digital currencies (…)".[67] These properties include quick transfers, the security of cryptography, and the ability to move funds across borders.

With regard to the trustworthiness of Facebook, a few questions about Libra's security arose. When Libra was first announced in 2019, Executive Director of the European Central Bank, Yves Mersch, argued that Libra is considered "cartel-like" and would be regulated accordingly.[68] He and other international authorities were critical of Facebook for having violated data protection legislation multiple times in the past, both in the United States and Europe. Mersch also claimed that only an independent central bank can provide the necessary support to demonstrate Libra's reliability and trustworthiness to the public.[69]

The European Central Bank was critical of Libra because although it had been designed to be centralized, it was going to be controlled by a conglomerate of private corporations that are held accountable by their shareholders, while the members of the Libra Association are only partially liable. Since there would have been no final creditor, the consequences of a potential liquidity crisis were unknown. Furthermore, the use of Libra raised legal questions concerning potential registration duties. Especially within the European Union, the policing of Libra could have proven to be difficult because the fundamental corporation is not based in the EU. The Libra Association cites Switzerland's openness toward financial innovation, its solid financial regulatory framework and its historic role as a platform for international organizations as reasons for its decision to be based there.[70] Due to the anticipated international use of the currency, transnational controls will be necessary. With regard to monetary policy, critics argued that Libra could influence the liquidity positions of banks and decrease the international significance of influential fiat currencies such as the euro.[71]

With regard to tech companies' collection of data, online privacy is becoming an increasing concern for consumers—particularly as it applies to Facebook. Therefore, many lawmakers have raised questions pertaining to the potential exploitation of user data with regard to Calibra, which is Libra's digital wallet.[72] U.S. Secretary of the Treasury, Steven Mnuchin, had stated that Libra might represent a national security risk, specifically with regard to money laundering.[73] Especially because the Libra

[67] Libra.org, *Libra White Paper,* https://libra.org/de-DE/white-paper/#the-libra-currency-and-reserve (last visited November 20, 2019).

[68] Steve Kaaru, *European Central Bank Exec Slams Libra as 'Cartel-Like,'* https://coingeek.com/european-central-bank-exec-slams-libra-as-cartel-like/ (last visited November 19, 2019).

[69] Steve Kaaru, *European Central Bank Exec Slams Libra as 'Cartel-Like,'* https://coingeek.com/european-central-bank-exec-slams-libra-as-cartel-like/ (last visited November 19, 2019).

[70] Libra.org, *Libra White Paper* (April 2020), https://libra.org/en-US/white-paper/?noredirect=1#cover-letter (last visited October 26, 2020).

[71] European Central Bank, Money and Private Currencies: Reflections on Libra – Speech by Yves Mersch, Member of the Executive Board of the ECB, at the ECB Legal Conference, Frankfurt am Main (September 2, 2019).

[72] Michael J. Casey, *Libra's Biggest Problem,* https://www.coindesk.com/libras-biggest-problem (last visited November 20, 2019).

[72] Ryan Browne*, Facebook's Libra Coin a Catalyst for Reform, Swedish Central Bank Chief Says,* https://www.cnbc.com/2019/10/15/facebook-libra-cryptocurrency-a-catalyst-for-reform-swedens-riksbank.html (last visited November 20, 2019).

[73] Bitcoin News Schweiz*, US-Finanzminister Steven Mnuchin: Facebooks Libra könnte für Geldwäscherei missbraucht werden,* https://www.bitcoinnews.ch/16282/us-finanzminister-steven-mnuchin-facebooks-libra-koennte-fuer-geldwaescherei-missbraucht-werden/ (last visited November 20, 2019).

Association has since vowed to make Libra compliant with AML and CFT standards and ensure that it is not used to circumvent sanctions, how Facebook will be able to ensure that its data protection policies, standards, and controls are enforced in all jurisdictions can be questioned.

Due to the extensive criticism, partly outlined above, the Libra Association has departed from its initial approach and published a new, revised *White Paper* in April 2020 to replace its original *White Paper* that had been published in June 2019. On one hand, the Libra Association will use distributed governance through Association Members and distributed technology to create an open system. Moreover, four key changes were introduced: Firstly, the Libra Association will offer single-currency stablecoins in addition to its originally planned multi-currency coin (Libra), meaning that the Libra network will allow its users to directly access stablecoins in their local currency, such as LibraUSD, LibraEUR, LibraGBP, etc. Secondly, a robust compliance network will be established, to ensure compliance with applicable laws and regulations while supporting financial inclusion and openness. This framework will include AML, CFT, sanctions compliance and prevention of illicit activities measures. Thirdly, the Association will forgo its initial plan to transition Libra to a permissionless system to ensure that unknown participants cannot take control of the system. In a permissionless system, no permission is required to become part of the network, transact, and validate transactions. Popular permissionless blockchains include bitcoin, ethereum, litecoin, monero, and dash. Peers in a permissioned blockchain need prior approval from a central authority. Lastly, the Association will build strong protections into the design of the Libra Reserve, including the maintenance of a capital buffer and holding assets with short-term maturity, low credit risk, and high liquidity.[74]

V. LEGISLATION

Countries that currently have blockchain regulations in place are the United States, Belarus, Malta, and Gibraltar.[75] Cryptocurrencies, on the other hand, are more frequently policed by governments. A distinction between direct and indirect regulation can be made. Whereas direct regulation consists of governmental laws governing blockchain-related technology, indirect regulation encompasses the rules that blockchain and tech companies have to follow.[76] Bitcoin, the most well-known application of blockchain technology, has been banned in 10 countries as of 2020. Ten countries have placed restrictions on Bitcoin and do not allow trading or payments to be made using Bitcoin. However, the countries that ban or restrict Bitcoin do not usually see a decrease in its usage or trade because decentralized cryptocurrencies can hardly be banned in one jurisdiction when they are legal in another.[77] Bitcoin is legal in 16 countries as of January 2020.

In myriad other jurisdictions, cryptocurrency is neither legal nor illegal. Among these "undecided countries" are Colombia, the Maldives, Jamaica, Kazakhstan, Argentina, and the United Arab Emirates.

[74] Libra.org, *Libra White Paper* (April 2020), https://libra.org/en-US/white-paper/?noredirect=1#cover-letter (last visited October 26, 2020).

[75] Darya Yafimava, *Blockchain and the Law: Regulations Around the World,* https://openledger.info/insights/blockchain-law-regulations/ (last visited November 20, 2019).

[76] Darya Yafimava, *Blockchain and the Law: Regulations Around the World,* https://openledger.info/insights/blockchain-law-regulations/ (last visited November 20, 2019).

[77] Cryptonews, *Countries Where Bitcoin is Banned or Legal in 2020* (January 2020), https://cryptonews.com/guides/countries-in-which-bitcoin-is-banned-or-legal.htm (last visited November 20, 2019).

These countries represent a particular threat to compliance efforts as there is no adequate legal framework in place for dealing with cryptocurrencies. Consequently, money launderers, terrorist financiers, and other criminals are drawn to exploiting this weakness for their own benefit.

A. FATF and the European Parliament

In June 2019, the Financial Action Task Force (FATF), which sets international standards in the fight against money laundering, published new guidelines for virtual asset providers (VASPs). These include the owners of crypto exchanges. Like "tokens," the term "virtual asset" describes a digital representation of a certain value which can be transferred, traded, or used for payment.[78] The providers of these virtual assets must do so in accordance with the FATF guidelines and collect extensive data in order to identify their customers. This data must be handed over to the authorities upon request. These new standards are considered highly controversial because they significantly restrict users' privacy. However, the regulations only apply to tokens, which have thus far not been regulated and have similar characteristics to other regular currencies.[79]

The guidelines were reviewed and revised in June 2020. The FATF revision report finds that both the public and private sectors have made progress in implementing the FATF standards and begun to either regulate or prohibit VASPs. Thirty-five out of 54 reporting jurisdictions had implemented the revised FATF Standards by July 2020. The FATF further concludes that the virtual asset sector required continued monitoring due to its "fast-moving and technologically dynamic" nature.[80] A second 12-moth review will be conducted by June 2021.[81]

Since January 10, 2020, EU member states have been obliged to implement the 5th EU anti-money laundering directive (AMLD5). According to the directive, service providers that exchange virtual currencies for regular fiat currencies and wallet providers are subject to due diligence. Due diligence includes strict KYC protocols and requires registration with the local authorities. At the same time, service providers have to monitor all transactions and report suspicious ones. In addition, national authorities, such as tax authorities, are permitted to access user information.[82]

B. Liechtenstein

Liechtenstein passed the so-called "Tokens and TT Service Providers Act (TVTG)" in October 2019. This blockchain act entered into effect on January 1, 2020. The law directly regulates blockchain-related services, making Liechtenstein a pioneer in blockchain regulation. With the TVTG, the Liechtenstein

[78] Government of Liechtenstein, Report and Application of the Government to the Parliament of the Principality of Liechtenstein Concerning the Creation of a Law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) and the Amendment of Other Laws, No. 54/2019, at 95.

[79] Anna Baydakova & Nikhilesh De, *All Global Crypto Exchanges Must Now Share Customer Data, FATF Rules,* https://www.coindesk.com/fatf-crypto-travel-rule (last visited November 20, 2019).

[80] FATF, *12 month review of revised FATF Standards —Virtual assets and VASPS* (July 7, 2020), https://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html (last visited October 26, 2020).

[81] FATF, *12 month review of revised FATF Standards —Virtual assets and VASPS* (July 7, 2020), https://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html (last visited October 26, 2020).

[82] Anna Baydakova & Nikhilesh De, *All Global Crypto Exchanges Must Now Share Customer Data, FATF Rules,* https://www.coindesk.com/fatf-crypto-travel-rule (last visited November 20, 2019).

government intends to resolve key legal questions relating to the token economy.[83] In the TVTG, particular attention is paid to TT service providers ("TT" stands for "trustworthy technologies" and is an abstract term for blockchain technologies)[84] because they represent a middle ground for the policing of blockchain users. Similar to banks, these service providers have to implement KYC and AML measures. Thus, they are likely able to uncover money laundering schemes and criminal activities. Moreover, the Duty of Care Act and other laws have been amended with regard to blockchain technology.[85]

C. Germany

In accordance with the AMLD5, Germany has been regulating crypto assets since January 1, 2020. While the directive mainly impacts fintech and industrial companies, it affects other businesses as well. Going forward, the safekeeping and trading of crypto assets will require a license from the German Federal Financial Supervisory Authority (BaFin).[86] Similarly, TT service providers in Liechtenstein are required to register with the Financial Market Authority (FMA).[87] One specific regulation within the cope of the AMLD5 has posed a particular challenge to companies: since January 1, 2020, service providers who offer the safekeeping of crypto assets have not been able to offer any other financial or banking services. Therefore, the businesses concerned had to establish subsidiaries. These require a separate license from the BaFin.[88] This process can be highly time-consuming and also costly.

[83] Government of Liechtenstein, Report and Application of the Government to the Parliament of the Principality of Liechtenstein Concerning the Creation of a Law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) and the Amendment of Other Laws, No. 54/2019, at 6.

[84] Government of Liechtenstein, Report and Application of the Government to the Parliament of the Principality of Liechtenstein Concerning the Creation of a Law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) and the Amendment of Other Laws, No. 54/2019, at 6.

[85] Government of Liechtenstein, Report and Application of the Government to the Parliament of the Principality of Liechtenstein Concerning the Creation of a Law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) and the Amendment of Other Laws, No. 54/2019, at 116–172.

[86] Philipp Sandner & Benjamin Schaub, Deutschland reguliert Krypto-Assets ab dem 1. Januar 2020: Was sind die besten Strategien für Blockchain-Startups, FinTechs, Banken, Krypto-Börsen und auch Industrieunternehmen?, https://medium.com/@philippsandner/deutschland-reguliert-krypto-assets-ab-dem-1-2211dff8ed72 (last visited November 20, 2019).

[87] Government of Liechtenstein, Report and Application of the Government to the Parliament of the Principality of Liechtenstein Concerning the Creation of a Law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) and the Amendment of Other Laws, No. 54/2019, at 85.

[88] Philipp Sandner & Benjamin Schaub, Deutschland reguliert Krypto-Assets ab dem 1. Januar 2020: Was sind die besten Strategien für Blockchain-Startups, FinTechs, Banken, Krypto-Börsen und auch Industrieunternehmen?, https://medium.com/@philippsandner/deutschland-reguliert-krypto-assets-ab-dem-1-2211dff8ed72 (last visited November 20, 2019).

D. United States

Cryptocurrencies are subject to extensive regulation in the United States; although laws may differ on the state level, on the federal level, cryptocurrencies are legal. In many places, they are even accepted as a form of payment. Federal agencies, like the U.S. Internal Revenue Service, the Commodities Futures Trading Commission, and the Securities and Exchange Commission, oversee blockchain-related companies. In their enforcement of regulations, these agencies frequently collaborate. Meanwhile, regulatory bodies have thus far paid little attention to blockchain technology and blockchain companies.[89] To tackle the issue, the Federal Trade Commission has formed a blockchain working group aimed at preventing fraudulent and illegal activities with the use of blockchain technology. Not only does the group regulate and discuss various blockchain matters, it also educates the public on the blockchain. With regard to blockchain technology and crypto regulation, experts argue that the United States is a global pioneer.[90]

E. Belarus

Belarus is an interesting case in terms of regulation because it not only welcomes but actively encourages the use of blockchain and cryptocurrency. In Belarus, the so-called "Digital Economy Development Ordinance" has been regulating the Hi-Tech Park (HTP) since March 2018. The HTP is frequently referred to as the Belarusian Silicon Valley. According to the decree, the HTP is a special sector that should be taxed separately, and it subjects the blockchain and cryptocurrencies to a legal framework.[91] Companies based in the HTP will be receiving a 100% tax break until 2023.[92] Moreover, HTP companies are not restricted in the storing, issuing, or trading of tokens. In addition to the decree, a blockchain law aimed at preventing terrorism financing, money laundering, and other criminal activities was passed in 2018.[93]

VI. IMPLICATIONS

With regard to international trade, many actors could benefit from the adoption of blockchain technology, and the technology has the potential to increase efficiency in trading processes.[94] With the adoption of blockchain technology, exporters could save both time and money. During a shipping process, for instance, numerous actors—including sellers, buyers, banks, and authorities—are

[89] Darya Yafimava, *Blockchain and the Law: Regulations Around the World,* https://openledger.info/insights/blockchain-law-regulations/ (last visited November 20, 2019).

[90] Darya Yafimava, *Blockchain and the Law: Regulations Around the World,* https://openledger.info/insights/blockchain-law-regulations/ (last visited November 20, 2019).

[91] Belarus News, *Digital Economy Development Ordinance,* https://eng.belta.by/infographica/view/digital-economy-development-ordinance-3071/ (last visited November 20, 2019).

[92] Iven DeHoon*, Belarus: 0% Tax for Blockchain Companies,* http://www.nomoretax.eu/belarus-zero-tax-for-blockchain-companies/ (last visited November 20, 2019).

[93] Ksenia Dobreva, *Belarus Passes New Blockchain and Crypto Regulations: What it Means for Business and the World,* https://openledger.info/insights/belarus-passes-new-blockchain-and-crypto-regulations/ (last visited November 20, 2019).

[94] Emmanuelle Ganne, Can Blockchain Revolutionize International Trade? 17 (2018).

involved. All parties must share data and documents peer-to-peer. These isolated processes are time intensive.

The handling of paper documents and making delivery via express couriers are both inefficient and expensive.[95] The employment of blockchain technology could represent an alternative that reduces paperwork and meticulously documents the individual stops in a supply chain. Thus, blockchain technology could significantly increase transparency, and this in turn engenders trust among all the parties involved.[96] However, international trade can only benefit from the advantages of the blockchain when a policy environment is established.[97]

With globalization, blockchain technology can only be established as a constant in international trade when it is universally employed. After all, it makes no sense for businesses to adopt blockchain technology if their international trading partners do not employ it as well. However, those who realize the potential of the blockchain could benefit from first-mover advantages and establish themselves as leaders in the industry. Due to the fact that many countries are (legally speaking) somewhat indifferent to blockchain technology, companies could be hesitant to enter the market, and rightfully so. Thus, it is necessary to establish international standards as soon as possible. Ultimately, the technology will not disappear. Instead, its significance and omnipresence are likely to increase even more. Outright bans on the technology do not usually make much sense, since private users, at least, find ways to circumvent them. At the same time, bans might motivate innovators, entrepreneurs, and developers to relocate to other jurisdictions, which will ultimately have a negative impact on economic growth.[98]

When it comes to money laundering, terrorism financing, corruption, and other criminal activities conducted with the use of blockchain technology and cryptocurrencies, compliance officers and prosecutors must be aware of the ways that criminals exploit the blockchain and cryptocurrencies to commit criminal offenses. The previously outlined methods are intended to give compliance officials an idea of how creatively criminals circumvent the existing measures. Only when sufficient international legislation is in place will these risks be minimized. Although regulating the blockchain itself would be difficult, legislators in different jurisdictions could use the Liechtenstein TVTG and the Duty of Care Act as guiding principles for the implementation of their own blockchain acts. Other jurisdictions that currently regulate the blockchain, such as the United States, could also be used as reference points.

VII. CONCLUSION

The blockchain is a distributed public ledger that facilitates peer-to-peer transactions without the interference of financial intermediaries. The most well-known application of blockchain technology is cryptocurrencies. However, it can be employed in many other areas as well, such as international

[95] SAP, *Blockchain – International Trade,* https://www.youtube.com/watch?v=-N_jAJyh8_E (last visited November 19, 2019).

[96] Emmanuelle Ganne, Can Blockchain Revolutionize International Trade? 39 (2018).

[97] Roberto Azevêdo, *Research Workshop on Blockchain (Remarks by DG Azevêdo),* https://www.wto.org/english/news_e/spra_e/spra248_e.htm (last visited November 20, 2019).

[98] Economic growth is driven by technology (and other factors). See: Prateek Agarwal, *What is Economic Growth*?, https://www.intelligenteconomist.com/economic-growth/ (last visited November 20, 2019).

trade. Generally, the blockchain is inherently highly transparent and secure due to its underlying technology. However, with cryptocurrencies, this transparency reaches its limits. In fact, decentralized cryptocurrencies like Bitcoin are known to be highly anonymous. As a result, they create a number of compliance risks, including their potential use in money laundering, terrorism financing, corruption, etc. At the same time, most decentralized cryptocurrencies are rather volatile in value. Stablecoins, on the other hand, are less volatile, but their compliance risks are similar to those of other cryptocurrencies.

Blockchain technology is omnipresent and unlikely to lose relevance in the future. On the contrary, the importance of blockchain technology for businesses and private market participants is likely to increase exponentially. Therefore, governments must begin to implement more adequate regulations. Ideally, an international standard should be set to serve as a guiding principle for all jurisdictions, especially since most businesses are currently unable to benefit from blockchain technology because of the lack of regulation. This uncertainty leads to legal gray areas, which businesses naturally avoid. The European Union, the FATF, and a number of individual states, such as Liechtenstein, have passed the first regulations on and guidelines for the usage of blockchain technology and cryptocurrencies. Although some aspects of these guidelines are considered controversial, they are necessary from a compliance perspective. Only when other jurisdictions follow their example will all actors be able to reap the benefits of the blockchain.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

THE CRIMINAL RESPONSIBILITY OF ASSOCIATIONS UNDER AUSTRIAN LAW

Bettina Caspar-Bures

AUTHOR

Bettina Caspar-Bures, LL. M., is working at the law firm Soyer, Kier, Stuefer since June 2014, where she is a registered lawyer since November 2018. She is specialized in criminal defence before domestic and international courts, criminal appeal proceedings, corporate crime, corporate compliance, financial criminal law, narcotics law, criminal law and media law, administrative criminal law and penitentiary law, as well as constitutional law and human rights.

Since July 2018, she has also been a member of the Austrian Ombudsman Board, which is responsible for the preventive control of torture and degrading treatment in facilities (=OPCAT) with measures that restrict freedom (prison, police detention center, nursing home, psychiatry, etc.).

Due to her several years of experience in one of the largest and leading law firms in the field of criminal and commercial criminal law in Austria, she has profound experience in legal theory as well as in practice in the field of corporate criminal law.

ABSTRACT

The Austrian Act of Corporate Criminal Liability came into force on January 1, 2006. Since then, associations can be penalized for judicially criminal acts of their decision-makers and / or employees. A criminal liability of the association presupposes that the offense was committed in favor of the association and, that the criminal offense violates the duties determined by the association (association duties).

In the case of a violation against the VbVG, the court will impose an association fine, which depends on the annual yield of the association. In addition, an instruction can be issued for compensation for damage.

In 2018 there were counted 341 preliminary investigations against associations, of which only 28 resulted in an indictment. Only in five cases, there was a conviction, and an association fine was imposed.

TABLE OF CONTENTS

I. INTRODUCTION OF THE AUSTRIAN ACT OF CORPORATE CRIMINAL LIABILITY

In 2005, the aim of the legislation was to remedy shortcomings in the fight against white-collar crime and thus also to take account of international legal developments, in particular European Union legislative acts, and obligations under international law, which required the introduction of effective, proportionate and dissuasive sanctions.[1] The responsibility of associations for criminal offenses was to be placed under criminal jurisdiction and thus therefore go further than European and international standards.[2]

Following a review phase, the National Council passed what is known as the Verbandverantwortlichkeitsgesetz (Austrian Act of the Corporate Criminal Liability, henceforth: VbVG) on September 28, 2005, which entered into force on January 1, 2006. The intention of the VbVG is, on the one hand, to sanction associations and, on the other, to create an incentive for prevention: The threat of (noticeable) fines is intended to increase awareness among companies of potential risks within their businesses and to promote the introduction of internal control and organizational mechanisms to prevent criminal acts by decision-makers and employees.[3]

II. ADDRESSEES OF VBVG

Until the introduction of VbVG, the concept of an association was foreign to Austrian criminal law dogmatics.

A. Definition of an association

According to the legal definition of § 1(2) VbVG, associations are *"legal entities as well as business partnerships and European economic interest groupings"*. The legal forms exhaustively listed have their (partial) legal capacity as a common denominator. VbVG is not based on a profitable or economic objective of the association, which is why associations with charitable or humanitarian objectives are also included.

[1] Second Protocol of June 19, 1997 of the Convention on the protection of the European Communities' financial interests (OJ 1997 C 221, 11); Directive 2003/6/EC of January 28, 2003 on insider dealing and market manipulation (OJ 2003 L 96, 16); CFD of July 22, 2003 on combating corruption in the private sector (OJ 2003 L 192, 54); CFD of February 24, 2005 on attacks against information systems (OJ 2005 L 68, 67); OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (BGBl III No.176/1999); Council of Europe Criminal Law Convention on Corruption of January 27, 1999 (ETS 173); UN Convention against Corruption (BGBl. III No 102/2002).

[2] The international and European legal obligations would also have been met if they had been anchored in administrative criminal law – EBRV (explanatory notes on the government bill) 904 BlgNr 22 GP 1; *Steininger*, Lehrbuch VbVG² Chap 1 Rec 24.

[3] EBRV 904 BlgNr 22 GP 1f; *Boller*, Die strafrechtliche Verantwortlichkeit von Verbänden nach dem VbVG, 19.

B. Circle of addressees

The addressees are thus both legal entities under private and public law and business partnerships.

1. Legal entities

Legal entities under public law include corporations such as stock corporations, limited liability companies and Societas Europaea, as well as cooperatives, idealistic associations, political parties and asset groups such as funds and foundations. Legal entities under public law are primarily local authorities (federal, state, municipality), economic and professional self-government institutions (chambers), social security institutions, universities, public law foundations and funds, but also the Oesterreichische Nationalbank. In spite of their legal personality, estates, sovereign acts by the federal government, state government, municipalities or other legal entities and the pastoral work of recognized churches, religious societies and religious denominations are expressly excluded from the scope of VbVG.[4]

2. Business partnerships

Business partnerships include OG (open societies) and KG (limited partnerships). They have the same legal capacity as corporations, but are not legal entities according to prevailing opinion and prevailing case law because the members are personally liable in addition to the corporate assets.

The scope of application of VbVG does not include sole proprietorships, civil law companies and silent partnerships as they are not legal entities and they do not have civil legal capacity.[5]

III. CRIMINAL LIABILITY

A. General theory of criminal law

Austrian criminal law is characterized by criminal law based on deeds. Punishment can only occur if there is guilt, which inevitably presupposes human action. In contrast to criminal law based on offenders, the focus is on the individual act and not the personality of the perpetrator. As associations never act themselves, they are not capable of forming their own will and are therefore never guilty in the classic sense.[6] The traditional principle of guilt was therefore not applicable to associations.

B. Responsibility of the association: Attributable persons

With VbVG, a new criminal law subject has been created, which has nothing to do with traditional criminal law as criminal law based on deeds and guilt, and thus human-based guilt.[7] The guilt of the

[4] *Steininger*, Lehrbuch VbVG² Chap 2 Rec 1ff.

[5] *Zirm* in *Hilf/Pateter/Schick/Soyer*, Unternehmensverteidigung und Prävention im Strafrecht, 68.

[6] *Steininger*, Lehrbuch VbVG² Chap 1 Rec 31.

[7] *Boller*, Die strafrechtliche Verantwortlichkeit von Verbänden nach dem VbVG, Foreword; *Steininger*, Lehrbuch VbVG² Chap 1 Rec 26.

association was not enshrined in VbVG, but its responsibility was standardized. This criminal liability of the association is linked to the criminal conduct of its decision-makers or employees.[8]

1. Decision-makers

Decision-makers are persons who have either power of (external) representation, control in a managerial position or a de facto influence on the management. Demonstratively named as decision-makers are the managing director, the board member, the authorized representative and the supervisory board member.[9] They are characterized by the fact that they carry and influence the will of the association, which means that they are regarded as the authors of the association's ethics. Persons who have only individual powers are not decision-makers unless the criteria of independent scope of action and supervisory and organizational responsibility are met in exceptional cases (see point 3.2.2.).[10]

2. Employee

Employees within the meaning of VbVG are all employees, who personally and economically dependent on the association, as well as persons who do not work in a personal but economic dependency (= employee similarity), as well as temporary workers and persons performing public service duties (= civil servants or contract workers). This exhaustive list of employee activities means that voluntary or honorary activities for the association can never fall under VbVG.[11]

The assessment of whether the deed was committed by a decision-maker or an employee must be based on the factual position in the association. If the person is formally in a managerial position but in reality does not have the power to make decisions, he is to be regarded as an employee.[12] If, on the other hand, the person formally performs employee activities, but actually has the power to make decisions (e.g. de facto managing director), he is to be treated as a decision-maker.

The misconduct of this natural person(s) is thus a prerequisite for the responsibility of the association, comparable to an "association-related guarantor status".[13] That is to say, decision-makers have a special legal duty of supervision. In teaching, the constitutional conformity of this criminal responsibility was initially[14] discussed. The Austrian Constitutional Court declared VbVG and the provision on responsibility (§ 3 VbVG) admissible on December 2, 2006. In its guideline ruling, it stated: *"The provision on the criminal liability of an association for the offenses of its decision-makers or employees does not violate the principle of objectivity and the right to a fair trial. As a criminal law category of its own kind, the association's liability cannot be measured against the principle of guilt."*[15]

[8] § 2 VbVG as amended.

[9] § 2(1) VbVG as amended; *Boller*, Die strafrechtliche Verantwortlichkeit von Verbänden nach dem VbVG, 128ff.

[10] *Zirm* in *Hilf/Pateter/Schick/Soyer*, Unternehmensverteidigung und Prävention im Strafrecht, 75f.

[11] § 2(1)(1) to (4) VbVG as amended; *Boller*, Die strafrechtliche Verantwortlichkeit von Verbänden nach dem VbVG, 142ff.

[12] *Steininger*, Lehrbuch VbVG² Chapter 5 Rec 42.

[13] *Steininger*, Lehrbuch VbVG² Chapter 3 Rec 1.

[14] The annulment of the entire VbVG, in the alternative § 3 VbVG, was requested with a party motion to the Constitutional Court.

[15] VfGH dated December 2, 2006, G 497/2015; JSt 2017, 50ff.

C. Responsibility of the association: Punishable offense

1. Type of criminal act

Associations can be held responsible for all acts against natural persons that are subject to judicial sanctions.[16] VbVG is neither limited to certain criminal offenses nor to certain types of offenses or forms of perpetration. Thus, both intentional and negligent offenses, crimes of omission and perpetrated offenses, and offenses of official and private prosecution are covered.

2. Conditions of criminal liability

The decisive factor is that the act was committed by a decision-maker or employee for the benefit of the association or the act violated obligations which affect the association. While the association is directly responsible for the culpable actions of the decision-maker, it may (only) be held liable for criminal acts of its employees if decision-makers have disregarded due and reasonable diligence and the perpetration was made possible or significantly facilitated by this.[17] There must therefore be organizational culpability and/or a violation of the supervisory duties of the association.

a. For the benefit of the association

An act is committed for the benefit of the association if the association receives a material advantage through the act, has thus been enriched or was spared economic expenditure.[18] However, non-asset offenses may also have been committed for the benefit of the association, such as forgery of documents or coercion. For the accountability of the association, it is not necessary that the natural person had the intention to grant an advantage to the association, but (only) requires its actual betterment. If the association is itself a victim of the offense committed by the natural person, it is not liable under criminal law because the misconduct typical of the offense is lacking.[19]

b. Breach of duty

The association is also responsible if it fails to take measures to prevent the offenses by its natural persons[20] and thus violates its obligations arising from the area of activity or responsibility of the association.[21] The relevant obligations are predominantly standardized in civil and administrative law (laws, regulations, decisions, etc.) and are particularly reflected in the form of road safety obligations, obligations for monitoring risks, product monitoring, warning and recall obligations, and obligations in the field of employee protection law, environmental law, construction law, trade law, etc.[22]

---

[16] RIS-Justiz RS0131120.

[17] § 3 VbVG as amended; EBRV 994 BlgNR 22. GP, 22.

[18] RIS-Justiz RS0131245.

[19] *Hilf/Zeder* in *Höpfel/Ratz*, WK² VbVG § 3 Com 1, Rec 10 and 12.

[20] *Zirm* in *Hilf/Pateter/Schick/Soyer*, Unternehmensverteidigung und Prävention im Strafrecht, 104.

[21] *Hilf/Zeder* in *Höpfel/Ratz*, WK² VbVG § 3 Rec 6.

[22] *Boller*, Die strafrechtliche Verantwortlichkeit von Verbänden nach dem VbVG, 161 ff; *Hilf/Zeder* in *Höpfel/Ratz*, WK² VbVG § 3 Rec 14; *Steininger*, Lehrbuch VbVG² Chapter 5 Rec 14.

3. Conclusion

The actions must therefore be sufficiently related to the association and its activities, and there must be sufficient links to the sphere of association.[23] Acts committed exclusively in the private interest of the natural person (= excesses) do not trigger criminal liability for the association.[24]

The criminal liability of the natural person and the association exist in parallel. A transfer to the association does not take place. A violation of the prohibition of double punishment ("ne bis in idem") must be denied because different subjects are sanctioned.[25]

IV. SANCTIONS

A. General

The intergovernmental acts of law called for *"effective, proportionate and dissuasive sanctions"* against legal entities. The creation of a monetary sanction was therefore mandatory, while the introduction of other sanctions was optional.[26] VbVG included the association's fine as the only independent sanction against the association. "Liability surrogates" such as bans on certain activities, the exclusion from public contracts or establishment closures have not been enshrined.[27] This was justified by the fact that secondary penalties are largely foreign to the Austrian criminal law system and that the division of duties between criminal law and administrative law should be maintained.[28] In teaching, the sanction system in VbVG is discussed very critically:[29] A successful fight against corporate crime would have required a more differentiated, more flexible sanction system,[30] from which something can certainly be gained.

B. Association fine

1. Calculation

As in the case of fines imposed on natural persons, the association's fine is to be calculated in daily rates. First of all, the number of daily rates should be determined on the basis of the severity of the accusation and then the amount of the daily rate on the basis of the economic performance of the association.

[23] EBRV 994 BlgNR 22. GP, 21.

[24] *Hilf/Zeder* in *Höpfel/Ratz*, WK² VbVG § 3 Rec 21.

[25] *Steininger*, Lehrbuch VbVG² Chapter 5 Rec 85.

[26] EBRV 994 BlgNR 22. GP 24; *Zirm* in *Hilf/Pateter/Schick/Soyer*, Unternehmensverteidigung und Prävention im Strafrecht, 141.

[27] *Steininger*, Lehrbuch VbVG² Chapter 6 Rec 1; EBRV 994 BlgNr 22. GP 27.

[28] EBRV 994 BlgNr 22. GP 27.

[29] *Schwarz/Steineder* in *Hilf/Pateter/Schick/Soyer*, Unternehmensverteidigung und Prävention im Strafrecht, 165.

[30] *Köck*, JBl 2005, 484ff; *Bauer,* ÖJZ 2004, 493; *Frank-Thomasser/Punz*, Unternehmensstrafrecht 14.

a. Number of daily rates

The number of daily rates depends on the framework for penalties for the natural person. It amounts to at least one and up to a maximum of 180 daily rates for deeds by the natural person, which are threatened with life imprisonment or up to twenty years' imprisonment.[31]

When assessing the penalty, the court must take into account both the special provisions of § 5 VbVG and the general principles of penal assessment, in particular aggravating and mitigating factors pursuant to §§ 32ff StGB. In contrast to individual criminal law, guilt cannot be the basis of the sanction when determining the penalty of the association,[32] which is why only those aggravating and mitigating factors are to be used that reflect their regulatory content in the structure of the association and not those that are linked to a certain character trait.[33]

§ 5(2) VbVG standardizes as reasons resulting in a higher number of daily rates, in particular (i) the amount of damage or risk, (ii) the amount of the (economic) advantage obtained, and (iii) the number of illegal acts. The latter is based on the action value of the breach of supervisory duty: The more grossly the decision makers have neglected their duties to monitor employees, the more the association has to be held responsible.[34] Relevant previous convictions would be regarded as aggravating, as in individual criminal law.[35]

§ 5(3) VbVG considers it a mitigating circumstance if the association (i) had already taken preventive measures before the offense was committed or has urged employees to act in accordance with the law, (ii) has taken significant steps towards future prevention, (iii) is only responsible for crimes committed by employees and not by decision-makers, (iv) significantly contributed to the establishment of the truth after the crime, (v) has made good the damage, or (vi) the act has already caused significant legal disadvantages for the association or its owners. When calculating the penalty, the behavior of the association following the offense must therefore also be taken into account, which expresses the admissibility of the internal investigation of criminal offenses within the company. If the association is responsible for a criminal offense, the association's cooperation with the prosecution authorities (if this contributes to the establishment of the truth) necessarily leads to a mitigation of the sanction assessment, which may even lead to a refusal to prosecute (see point 5.2.3.)[36]

b. Amount of the daily rate

The amount of the daily rate is calculated according to the profit situation of the association. The daily rate is fixed at the 360th part of the annual yield, with no specific period of calculation defined. The basis of calculation can therefore be both the annual yield of the last business year and an average view of the last few years.[37]

[31] § 4(3) VbVG as amended.

[32] EBRV 994 BlgNR 22. GP 27; *Steininger*, Lehrbuch VbVG² Chap 6 Rec 4.

[33] *Steininger*, Lehrbuch VbVG² Chap 6 Rec 4 and 9f.

[34] *Steininger*, Lehrbuch VbVG² Chap 6 Rec 13.

[35] EBRV 994 BlgNR 22. GP 28; cf. § 32 Z 2 StGB as amended.

[36] *Madl* in *Kert/Kodek*, Das große Handbuch Wirtschaftsstrafrecht, 22.31; § 5(3)(3) and § 18 VbVG as amended.

[37] *Fabrizy*, StGB- Nebengesetze[11], VbVG § 4 Rec 2; *Hilf/Zeder* in *Höpfel/Ratz*, WK² VbVG § 4 Rec 12.

Earnings are defined as the amount available to the association after necessary investments and borrowing costs and after deducting all taxes, i.e. the amount which the association could freely dispose of. The determination of earnings is not based on any defined criteria, as there are different tax regulations for the associations (profit and loss account, balance sheet, international accounting rules, etc.). In any case, no reference is made to figures such as turnover, profit before tax or other tax bases.[38] This was justified by the fact that a punishment was to be achieved while at the same time preventing a threat to the operating basis.[39]

The system, which ties in with the profit situation and only marginally considers other economic performance, is viewed very critically in teaching.[40] In my view, this is to be endorsed. The regulation leads to an improvement in the position of those companies that are financially strong and have high turnover, but often have low profits or revenue. This better position is further strengthened by the enshrining of a maximum daily rate limit in VbVG. A focus on turnover, as in EU antitrust law, would be a more accurate and fairer method in my opinion.

2. Minimum sentence

In addition to the maximum limit, VbVG also standardizes a minimum number of daily rates and the minimum amount of the daily rate, thereby imposing fine sanctions on associations that make losses: The daily rate is at least EUR 50.00 and a maximum of EUR 10,000.00 and, for associations with a non-profit, humanitarian or church purpose, at least EUR 2.00 and a maximum of EUR 500.00.

Therefore, the minimum penalty for associations is EUR 50.00, the maximum penalty is EUR 1,800,000.00 or, for associations with a non-profit, humanitarian or church purpose, at least EUR 2.00 and a maximum of EUR 90,000.00.

C. Association fine: conditional leniency

Like individual criminal law, VbVG also provides for the full or partial leniency of the penalty.

If it is assumed that the threat of the penalty will be sufficient to prevent the association from committing further acts for which it is responsible (= special prevention), nor does it require the enforcement of the fine to prevent the perpetration of acts by other associations (= general prevention), the enforcement of the association's fine is to be (partially) conditionally reviewed.

Leniency must be combined with a probationary period of one to three years. [41] It may also be accompanied by a directive requiring the consent of the association. [42] As a directive, VbVG

[38] *Zirm* in *Hilf/Pateter/Schick/Soyer*, Unternehmensverteidigung und Prävention im Strafrecht, 144.

[39] *Steininger*, Lehrbuch VbVG² Chap 6 Rec 30.

[40] *Schwarz/Steineder* in *Hilf/Pateter/Schick/Soyer*, Unternehmensverteidigung und Prävention im Strafrecht, 144f; Köck, JBl 2005, 485; Kern, SWK 2006, 469).

[41] §§ 6, 7 VbVG as amended; *Steininger*, Lehrbuch VbVG² Chap 6 Rec 41.

[42] EBRV 994 BlgNR 22. GP 29.

standardizes the obligation to provide compensation for damages or measures to improve corporate culture and thus to prevent damages in the future.[43]

As part of the sentence, the granting of leniency must be included in the judgment.[44] It may be revoked if a renewed conviction occurs within the probationary period or directives are not followed despite a formal warning.[45]

D. Civil law aspects of the association fine

While individual criminal law provides for a substitute sanction in the form of a substitute custodial sentence in the event of uncollectability of the fine, there is no such possibility in VbVG. If an association is unable to pay, this ultimately leads to bankruptcy or insolvency, where fines for criminal acts of any kind cannot be claimed.[46]

The association, which is held liable by the court under VbVG, cannot transfer the imposed sanction to the natural person. Civil law recourse is expressly excluded in VbVG.[47]

V. PROCEEDINGS

A. Principles of the proceedings

The general rules on criminal proceedings also apply to proceedings against the association, insofar as they do not relate exclusively to natural persons.[48] The provisions on the preliminary proceedings[49], the distribution of responsibilities[50], the prosecution[51], the main proceedings[52] and appeal proceedings[53] are thus also applicable to the proceedings on the liability of associations.

The preliminary, main and appeal proceedings against the association should, in principle, be conducted together with those against the natural person. The aim of this is to take into account economic and commercial aspects as well as to avoid the risk of contradictory results of evidence or the assessment of evidence. The conducting of the proceedings separately as an exception is

[43] § 8 VbVG as amended; *Schwarz/Steineder* in *Hilf/Pateter/Schick/Soyer*, Unternehmensverteidigung und Prävention im Strafrecht, 155.

[44] § 6 VbVG as amended; § 260(1)(3) StPO as amended.

[45] § 9 VbVG as amended.

[46] *Schwarz/Steineder* in *Hilf/Pateter/Schick/Soyer*, Unternehmensverteidigung und Prävention im Strafrecht, 151.

[47] § 11 VbVG as amended.

[48] § 14(1) VbVG as amended.

[49] cf. §§ 89ff StPO supplemented by § 13ff VbVG as amended.

[50] cf. §§ 25ff supplemented by § 14 VbVG as amended.

[51] cf. §§ 212ff, 451, 484 StPO supplemented by § 21 VbVG as amended.

[52] cf. §§ 228ff StPO supplemented by § 17 and §§ 22ff VbVG as amended.

[53] cf. §§ 280ff StPO supplemented by § 24 VbVG as amended.

conceivable in constellations in which no natural person could be determined as a perpetrator or cannot be prosecuted, e.g. because they are deceased, a fugitive or unfit to stand trial.[54]

The association is not capable of litigation, i.e. it cannot independently express itself in court as a party to the proceedings, participate in the proceedings and influence the proceedings.[55] For this purpose, the association requires representation by a body authorized to represent it, which is not itself a suspect. If all members of the body authorized to represent the association externally are suspected of having committed the offense, the court must appoint a defense counsel as a "collision curator". The collision curator must take the necessary steps to ensure proper representation of the association and will endeavor to appoint a representative who is not a suspect.[56]

B. Preliminary proceedings

1. Defendants´ rights

As the subject of the proceedings, the association is entitled to the rights of the accused. Thus, like the accused natural person, he has the right to defense, to information, to inspect files, to be heard, to participate in the taking of evidence, to submit requests for evidence, to observe the presumption of innocence, and to lodge an appeal.[57] His representation benefits from the right to refuse to testify and the ban on self-incrimination.

The decision-makers of the association are also accused in the proceedings against the association, irrespective of whether they are suspected of having committed a crime. In the case of employees, it is (only) those who are themselves suspects.[58]

2. Other measures

The provisions of StPO on enforcement measures in the preliminary proceedings also apply to associations. They are supplemented by the possibility of an interim injunction.

a. Enforcement measures

Under the same conditions as against the natural person, a house search, account information and account opening, securing, seizure, etc. can be ordered against the association.

b. Interim injunction

If a prosecuted association is urgently suspected of being responsible for a certain offense and it is assumed that a fine will be imposed on it, the court may, at the request of the public prosecutor's

[54] EBRV 994 BlgNR 22. GP 32; *Czerny/Oberlaber*, Zum richtigen Umgang mit dem VbVG, ÖJZ 2019, 306.

[55] *Markel* in *Fuchs/Ratz*, WK StPO § 1 Rec 24.

[56] § 16 VbVG as amended; Necessary steps include informing and/or convening the board of directors and/or general meeting. *Czerny/Oberlaber*, Zum richtigen Umgang mit dem VbVG, ÖJZ 2019, 309.

[57] *Hauser* in *Hilf/Pateter/Schick/Soyer*, Unternehmensverteidigung und Prävention im Strafrecht, 249.

[58] § 17 VbVG as amended.

office, order seizure to secure the association's fine. The prerequisite is that, due to certain facts, there is a fear that the collection of the fine would otherwise be endangered or made considerably more difficult.[59] There is therefore a real fear of malversation, such as the transfer of assets abroad. A merely emerging deterioration in earnings does not justify an interim injunction.[60]

3. Elimination of criminal liability

The ability to prosecute the natural person and the association in proceedings must be assessed separately. The association must also be given credit in the event of grounds for exemption from and suspension of punishment of the statute of limitations, abandonment of an attempt to commit an offense, active repentance, lack of criminal liability or self-denunciation in criminal financial law for the natural person, but not their death.[61] However, if the reason for the statute of limitations is an inhibiting circumstance on the part of the association but not on the part of the natural person or vice versa, the period will expire or continue separately.[62] In addition, the association can also fulfill substantive reasons for exemption from punishment independently of the natural person, as, for instance, only the association practices active repentance.[63]

4. Termination of preliminary proceedings

The preliminary proceedings are terminated by suspension, diversion, refraining from prosecution or application for the imposition of an association fine.

a. Diversion

The possibility of diversion and thus the alternative response to illegal conduct without conviction also exists in proceedings against associations. The public prosecutor's office must withdraw from the prosecution if (i) the facts have been sufficiently clarified; (ii) there is no jurisdiction of the court of lay assessors or jury court; (iii) the act did not result in the death of a person, and (iv) no general or special preventive reasons speak against it. As a diversionary service, VbVG provides for the payment of a monetary amount, the determination of a probationary period, as far as possible and appropriate in connection with an explicit willingness of the association to take preventive measures or the provision of a non-profit service. In contrast to individual criminal law, the criterion of guilt is not applicable due to a lack of individual decision-making. On the other hand, the diversion against the association necessarily presupposes that the damage caused by the offense has been made good and that other consequences of the offense have been eliminated and proven.[64] If the conditions for diversion are not met, the ordinary proceedings will continue.

[59] § 20 VbVG as amended; *Steininger*, Verbandsverantwortlichkeitsgesetz § 20 Rec 4.

[60] *Steininger*, Verbandsverantwortlichkeitsgesetz § 20 Rec 4.

[61] EBRV 994 BlgNR 22 GP 22.

[62] RIS-Justiz RS0132555.

[63] *Steininger*, Lehrbuch VbVG² Chap 1 Rec 37.

[64] § 19 VbVG as amended; *Schwarz/Steineder* in *Hilf/Pateter/Schick/Soyer*, Unternehmensverteidigung und Prävention im Strafrecht, 160.

b. Refraining from prosecution

In the prosecution of associations, the public prosecutor's office is granted discretion that has not been regulated to this extent in the Austrian (criminal) legal system.[65] While in individual criminal law the public prosecutor's office is, in principle, obliged to prosecute, the public prosecutor's office can refrain from prosecuting associations if a consideration of the severity of the offense, a consideration of the breach of duty or the breach of due diligence, the consequences of the offense, the behavior of the association after the offense, the expected amount of a fine to be imposed on the association as well as any disadvantages already incurred or directly foreseeable for the association or its owners resulting from the offense make prosecution and sanctioning appear unnecessary. The discretion is limited if the prosecution is necessary for special or general preventive reasons or because of a special public interest. [66]

C. Main proceedings

The jurisdiction of the procedure is based on the provisions for the natural person; there is no special jurisdiction. The main proceedings can therefore take place both before the district court and the regional court as a single judge, court of lay assessors or jury court.[67]

The main proceedings against the natural person begin with the filing of the criminal complaint or the indictment, those against the association with the (connected) application for the imposition of an association fine by the public prosecutor. Depending on the jurisdiction, the application must contain the formal requirements of the criminal complaint or the indictment.[68]

While the procedure of taking evidence should, in principle, be conducted jointly, the closing statements and the pronouncement of judgement must be conducted separately, initially against the natural person. If the proceedings against the natural person are terminated with a conviction, the closing statements and the verdict for the association will be held in a continuing main proceeding. If the proceedings against the natural person end with an acquittal, the public prosecutor's office must issue a (renewed prosecution) declaration within three days in order to continue the main proceedings against the association. If this declaration is not issued, this is equivalent to a withdrawal of the application and the court must acquit the association.[69]

The court has to make two independent judgments and also issue them separately.[70] If the court is of the opinion that no conviction is necessary to prevent the association from further criminal acts and if the other conditions for a diversion are met (see point 5.2.3.), it will (provisionally) discontinue the proceedings by order.[71]

---

[65] *Konopatsch* in *Hilf/Pateter/Schick/Soyer*, Unternehmensverteidigung und Prävention im Strafrecht, 172.

[66] § 18 VbVG as amended.

[67] *Grohmann/Scheck* in *Hilf/Pateter/Schick/Soyer*, Unternehmensverteidigung und Prävention im Strafrecht, 270.

[68] §§ 210ff StPO as amended.

[69] § 22(3) VbVG as amended; EBRV 994 BlgNR 22. GP 37.

[70] § 22(1) VbVG as amended; RIS-Justiz RS0130765; *Hauser* in *Hilf/Pateter/Schick/Soyer*, Unternehmensverteidigung und Prävention im Strafrecht, 229.

[71] *Czerny/Oberlauber*, Zum richtigen Umgang mit dem VbVG, ÖJZ 2019, 308.

In addition to the association's fine, as well as in individual criminal law, the court may declare confiscation according to § 20 of StGB. While the confiscation serves to take away the advantage gained by the offense, the association fine is the sanction for illegal behavior. Association fines and confiscation can therefore – without violating the prohibition of double punishment – be imposed side by side and independently of each other.[72]

Convictions of associations are included in the register of associations, which is maintained by the public prosecutor's office for the prosecution of white-collar crime and corruption. The register is accessible to the authorities but is not publicly accessible.

D. Appeal proceedings

The appeals and legal remedies provided in StPO are available against judgments concerning the association. The association can appeal against its decision as well as against the conviction of the natural person, if a precondition of its responsibility is derived from it.[73]

VI. FINAL REMARK

VbVG is discussed extensively in teaching. In practice, however, despite increasing numbers, it still has little significance in Austria: In 2009[74], two cases were settled by the public prosecutor's office and seven by the courts[75]. In 2018[76], 341 cases were settled by the public prosecutor's office and 24 by the courts. The majority of these 252 cases ended with a dismissal by the public prosecutor's office, only 28 charges were brought and only five cases were convicted. A diversion occurred in 14 cases. These figures compare with a total of 318,627 proceedings against natural persons in 2018.[77]

This reveals the still limited scope of VbVG and consequently few criminal sanctions against associations.

[72] EBRV 994 BlgNR 22. GP 30; *Soyer*, AnwBl 2005, 12.

[73] *Hilf/Zeder* in *Höpfel/Ratz*, WK² VbVG § 24 Rec 1; EBRV 994 BlgNR 22. GP 32.

[74] In 2009, proceedings against associations were included for the first time in the annual Security Report of the Federal Ministry of the Interior.

[75] Security Report of the Federal Ministry of the Interior 2015, 31.

[76] The latest published Security Report of the Federal Ministry of the Interior concerns 2018.

[77] Security Report of the Federal Ministry of the Interior 2018, 31 and 33.