orrick

VENTURE FINANCINGS AND EXPANSION PROJECTS IN THE UNITED STATES

GO WEST.

Practical Guidelines for German Technology Companies

2nd Edition

Acknowledgements

Many of our colleagues from our technology teams in Germany and the United States have shared their experiences with us, challenged our thinking and helped develop the concepts laid out in this Guide. Among the many valuable contributors were *Markus Piontek*, *Vanessa Sousa Höhl* and *Johannes Rüberg* from our Düsseldorf office, and *John Harrison* from our Silicon Valley office as well as *Jonathan Chou* from our New York office.

The authors would also like to thank our great research teams both in our German and U.S. offices, most notably *Lars Wöhning* and *Justine Koston*, for their valuable contributions to this project.

Finally, the authors extend their gratitude to *Nuno Teixeira* for his great support with designing this Guide.

Version: September 2018

CONTENTS

orrick

INTRODUCTION

This Guide will help founders of, and investors in, German technology companies seeking to raise capital from U.S. investors or simply to expand into the U.S. market. Our Orrick partners put it in *Atomico*'s insightful report *The State of European Tech – 2017*: "The times are-a-changing. Traditionally, European companies looking to be acquired have looked to Silicon Valley for their salvation. Today, they're looking to the U.S. as a destination to acquire, demonstrate their success or to expand internationally."

We have dedicated technology lawyers in all major world markets who support young German technology companies on their growth trajectory through all stages. As one of the top tech law firms in the world, we are particularly committed to bringing the United States and German entrepreneurship ecosystems closer together. We especially want to help German technology companies be attractive for American investors and scale in the U.S. market. To that end, throughout this Guide we will take the perspective of a potential U.S. investor and give helpful tips to founders and early stage investors of a German technology company to keep its financeability (*i.e.*, the ability of a company to raise future financing rounds) and attractiveness for potential later-stage American investors.

We will give helpful tips on when and how to look for a U.S. investor and discuss key differences between funding rounds in Germany and the United States. We will also examine the benefits and challenges of "flipping" a German GmbH into a U.S. company, often considered a cornerstone in developing a successful "Silicon Valley story." Given that the Delaware, Inc. is the most popular legal entity to choose for German entrepreneurs, we will provide a brief overview of the basics of a typical VC-backed Delaware, Inc.'s corporate (governance) structure.

Many German technology companies cannot afford to ignore the U.S. market and will sooner or later consider having a presence "on the ground." A U.S. market presence can help to achieve scale more quickly and help the company gather important market intelligence or to tap into rich(er) talent and technology pools. A U.S. presence will also often help to attract U.S. investors. Thus, in the second part of this Guide, we will discuss some operational topics for entering the U.S. market, ranging from protecting intellectual

property rights in the United States, privacy considerations when transferring personal data from and to the United States to key employment matters and participation programs in the United States and how to make typical German programs work for U.S. beneficiaries. We will also discuss some areas of law that are, especially when compared with the German market, specific for the U.S. market but of great importance for any foreign technology company coming to the U.S., including trade secrets and how to manage litigation risks.

Throughout this Guide, we toss in sidebars covering certain topics in greater detail and also giving guidance on some non-legal matters.

By necessity, this Guide will not be appropriate for every financing round and expansion project, as each company and every U.S. market entry is different. This Guide cannot substitute proper advice by a qualified lawyer on a case-by-case basis.

We hope you enjoy this Guide. If you would like to discuss it further, please get in touch. We would also love to learn about your experiences with these topics.
So please share them with us.
We constantly strive to evolve and grow in order to best serve our clients.

On behalf of the Orrick Team,

Sven Greulich
Orrick – Technology Companies Group Germany

U.S. VENTURE FINANCINGS FOR GERMAN TECHNOLOGY COMPANIES


TURN TO CLEAR VISION
QUARTERS ONLY
50¢
TO OPERATE
TURN
HANDLE
ONE
FULL
TURN

1. WHEN LOOKING FOR U.S. INVESTORS

As the U.S. and German tech ecosystems become more closely connected, raising capital in the U.S. market is becoming a strategic consideration for many fast-growing German tech companies. For some, establishing a presence in one of the U.S. tech centers will be a key inflection point.

THE ATTRACTIVENESS OF THE U.S. VENTURE CAPITAL MARKET

With our global platform across many of the world's tech hubs, we regularly work with German entrepreneurs and start-ups looking for funding from U.S.-based venture capital and corporate venture capital investors. Although it is certainly still a steep uphill climb for non-U.S. start-ups to obtain funding from most U.S. investors when coming into the U.S. market, we have seen increasing investment activity in European and, particularly, German start-ups over the last few years. This view is supported by data published by *PitchBook* in its Q1/2018 European Venture Report according to which U.S. investors continue strong showing in Euro financings with more than 22% of all European financing rounds and approx. 19.4% of all German financing rounds involving U.S. investors.

There are a number of trends leading us to believe that U.S. investments in German companies will continue to gain momentum, including:

- The maturing entrepreneurial ecosystem in Germany;
- The lower price tags for German start-ups and top-notch developer teams outside the U.S.; and
- The expected reallocation of investment dollars that had been earmarked for European start-ups following the Brexit to Germany.

With financing rounds by European investors in most cases still remaining substantially smaller than U.S. financing rounds for comparably mature emerging companies, it remains a very attractive (and sometimes the only) option for a German start-up to build its business in Germany, raise some money (often a super seed round or a (pre-) series A round) in Germany, use the proceeds to build up some traction in the United States and then go after a much larger later stage round in the United States.

With their extensive operational experience, financial firepower, roll-out and support capabilities to assist their portfolio companies, such smart money from U.S. investors can be very attractive.

Based on our experiences, we have summarized a few tips for German start-ups to increase their chances of landing a U.S.-backed financing.

FIND YOUR ACCESS POINT

German start-ups should be aware that they are facing stiff competition. With their networks in Silicon Valley and other major tech hubs such as New York and Boston, U.S. investors are sitting at the epicenter of the world's biggest entrepreneurial ecosystem (we know… with the notable exceptions of Tel Aviv, London, Berlin and increasingly the innovation clusters in China). This system is self-sustaining due to, amongst others, positive selection patterns as the best founders and companies tend to gravitate to them. Add the natural bias for home markets and it becomes clear how hard it is for an outsider to stand out.

Any U.S. investor will ask why a German start-up is not seeking funding in its home market. Especially early-stage investments in a start-up that is not already on the ground in the United States are difficult to pull off.

Building Networks – Orrick's Total Access Events

An excellent way for international founders to build their networks in the tech centers on both the East Coast and West Coast is Orrick's highly regarded Total Access Events Series. These events provide entrepreneurs business, tactical, legal education and coaching. Presented by experienced industry CEO's, venture capitalists and Orrick lawyers, Total Access offers insights on cutting-edge issues and an opportunity to network with leading professionals in the start-up community. Access is free.

To learn more about the current program and to make sure you get an invitation go to www.orrick.com/Total-Access.

U.S. investors will often request a minimum of U.S. traction. There needs to be trust right from the start, especially when there is little geographical proximity between investor and start-up (remember that many angel investors from Silicon Valley invest only in companies they can reach in sixty minutes or less).

To overcome these barriers and get in front of U.S. investors, the founders need to be on the ground and find their way into the investors' networks. Here, we recommend concentrating on investors that already have a proven track record of investing in European start-ups, preferably German start-ups, as for some U.S. investors the step from investing in a U.K. or Irish start-up into one from Continental Europe still seems to be a big one.

Sending out a blast email with a pitch deck to a bunch of investors is not a particularly promising strategy in Germany and is less so in the United States. Make no mistake, unsolicited pitches sent to an investor are most certainly deleted unread (there are simply too many) and, especially in early stages, engaging paid financial intermediaries (placement agents or "finders") to help generate leads is considered a waste of (investors') money and simply signals immaturity and naivety. Founders should spend time and energy developing and maintaining relationships with important players early on and seek a solid referral to an investor from someone in the investor's trusted network. For many investors, the first screening criterion is the effectiveness and creativity in which the prospect obtained an intro. Ultimately, one of the key jobs of the CEO of a start-up is getting to know investors and persuading those investors that she[1] is worth backing. Because venture capitalists are busy, with ever-changing schedules, this can be a frustrating exercise for those who are not on the ground.

It is often also advisable to get a smaller (German) venture capitalist with good ties to larger U.S. venture capitalists as a bridge builder, demonstrated by a solid track record of follow-on investments by its network partners, into the cap table in an earlier financing round. Although other investors might offer what seems to be more favorable terms, winning such an investor sends a powerful signal and can help a young German technology company overcome the liability of newness in the U.S. funding market.

COME PREPARED

When pitching to U.S. investors – this holds true both for venture capital and corporate venture capital investors – preparation tops zeal. Bear in mind that the renowned investors have to screen at least hundreds and often thousands of ideas every year. With time at a premium, it is imperative for each German start-up to come prepared and make it as easy as possible for a potential investor to check the boxes.

We are often asked if this means that a German start-up has to swap into a U.S. legal form (the famous "Flip," see Chapter A.2 below). Well, it depends. While some U.S. investors still only do investments in U.S. companies or at least have a strong preference for U.S. companies, over the last years we noted a change in attitude. Many U.S. investors today are not "afraid" of investing in a German Limited Liability Company (*Gesellschaft mit beschränkter Haftung – "GmbH"*) any more (though, as we will see, there might still be other good reasons for a Flip).

But even with their start-up organized as a GmbH, German founders can make life easier for their prospective U.S. investors. If attracting U.S. investors is a serious prospect, founders should ensure that the shareholders'

1 Although only the female form (she) is used throughout this Guide to make it easier to read, any reference to the female gender shall also include all other genders.

and other agreements they enter into with their early stage investors and co-founders meet what a later stage U.S. investor would expect in a typical U.S. deal, *e.g.* typical preference rights and the flexibility to pursue further financing rounds and exit options (for a summary of typical U.S. deal terms see Chapter A.3 below).

When trying to entice U.S. investors with the potential of the U.S. market for the German start-up's product, it is also crucial that the start-up has conducted at least a basic compliance check of its product with U.S. regulations and that with the help of a qualified U.S. counsel a comprehensive IP strategy has been developed to ensure that the company has and retains essential IP rights (for more on this, see Chapter B.2 below).

A PITCH IS NOT A THEATER PLAY WITH AN UNFAIR ADVANTAGE FOR NATIVE SPEAKERS

When speaking at conferences or working with German entrepreneurs, it is surprising how often we hear that German entrepreneurs face a disadvantage because they can't pitch like their U.S. peers. Granted, American entrepreneurs don't have to overcome the language barrier. And it certainly helps any entrepreneur to take a page out of Y Combinator's playbook when preparing their start-ups for demo day. But, pitching is not a theater play. Some excitement can be contagious, but don't force it. While having a catchy soundbite prepared for investors to remember you is certainly a good idea — think of Ridley Scott's pitching the idea for his first Alien movie as "*Jaws on a Spaceship*" — trying to squeeze the maximum number of "disrupt" and "game changing" in an onslaught of technical jargon is certainly not.

What U.S. investors are looking for is evidence that there is a real customer need and market opportunity with growth potential, a strong team that can execute, an exit strategy and, as should have become clear from the above, a good reason why the German start-up seeks U.S. investors. Keep in mind that many U.S. investors need to deploy funds much larger than their European peers, so prepare for the question "how big can this be" and understand fund economics[2].

2 You may find some inspiration in an article entitled **"How to Impress a Venture Capitalist: 12 Prominent VCs Share What Gets Their Attention"** that our friend and former Orrick partner Richard Harroch — who is now with VantagePoint Capital Partners — published in *Forbes* (available online).

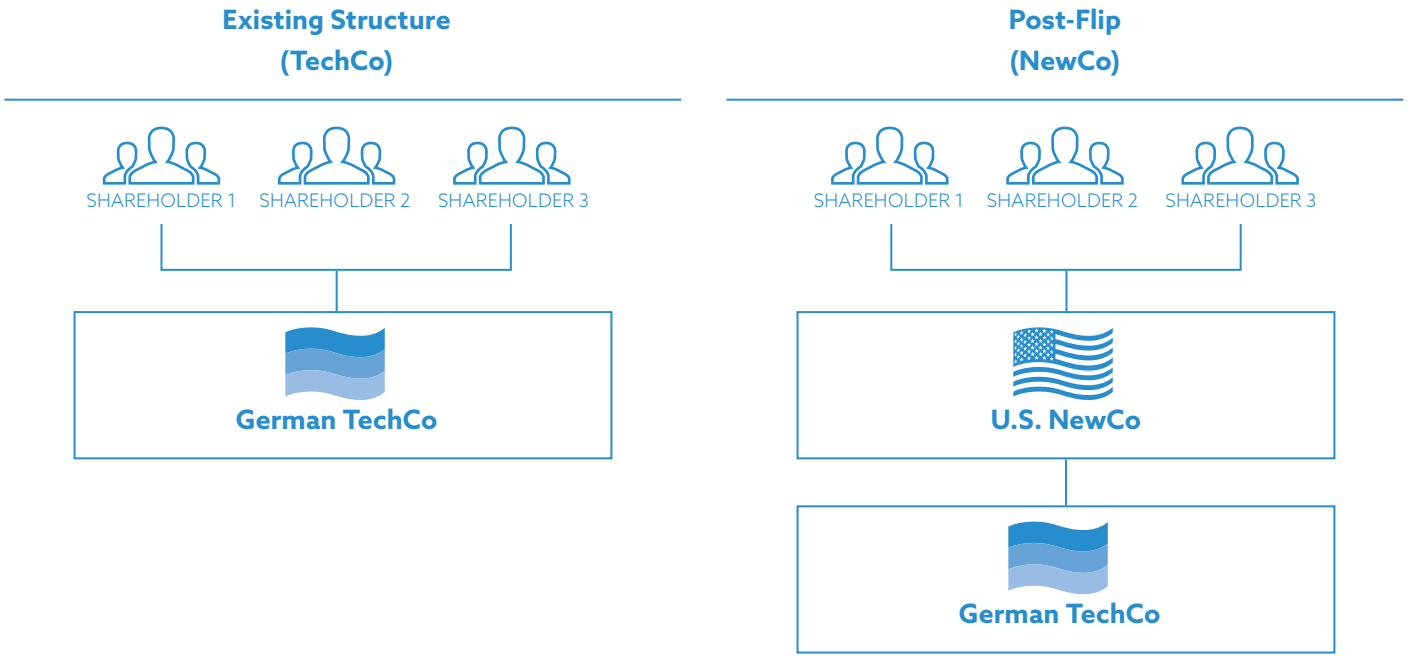
2. FLIPS – HOW TO BECOME A U.S. COMPANY

Many German technology companies are initially set up as a GmbH or its "little sister" the UG (haftungsbeschränkt) in which the founders, angels and maybe first institutional financial investors acquire a stake (either directly or through personal holding companies). As we will see, once the start-up has somewhat matured it may become an attractive option to change this initial corporate set-up and "flip" it into a U.S. company.

WHAT IS A FLIP?

A "Flip" refers to the "transfer" of a German start-up to a U.S. legal structure. In this process, the shareholders "swap" or "flip" their shares in the business-carrying German company ("TechCo") for shares in a U.S. company (often a Delaware Inc., "NewCo").

As a result, between the founders and TechCo, a new parent company is established: while NewCo becomes the new parent company in which incoming investors would invest, TechCo becomes a subsidiary.



Usually, intellectual property rights and employees remain with TechCo while NewCo assumes the role of a holding and management company that sometimes also enters into business relationships with customers in the United States (though for various reasons, it is often more advisable to establish another new U.S. company beneath NewCo, *i.e.* a sister company to TechCo, to act as operating company in the U.S. market).

MAIN REASONS FOR A FLIP

- Improved access to U.S. venture capital markets.
- Going public in the United States is much easier.
- Higher valuation of the company due to the "Silicon Valley story".
- Easier access to rich U.S. talent pool with U.S.-style ESOPs.

REASONS FOR A FLIP

Access to Investors: A central motive for the Flip is that in many cases the start-up will receive improved access to the significantly more liquid U.S. venture capital markets. The U.S. has 7 of the top 20 start-up locations worldwide, with Silicon Valley being number 1. The only German location is Berlin as number 7 (figures taken from the 2017 Global Startup Ecoystem Ranking published by the Global Startup Genome Project).

The United States has a higher number of potential investors, has a much more vibrant and developed venture capital scene, and has a higher disposition to invest, especially in riskier ventures than Germany or Europe. Also due to deeper sectoral diversification, investors may sometimes offer better know-how, contacts and guidance for the newcomer.

Moreover, by operating through a domiciled U.S. company, consisting formal investment restrictions may cease to apply, *e.g.* institutional investors may be prohibited by their charters from investing in and buying securities of non-U.S. companies.

Valuation and Exit Options: Start-ups with a "Silicon Valley story" also tend to receive higher valuations in future financing rounds and in exit scenarios. With a rather flat German IPO market, in particular for young technology companies, going public on NASDAQ or NYSE is an appealing alternative. In the U.S., an initial public offering (IPO) is often seen as a significant step in the maturation of a business from a small start-up stage to a successful operating company. In the now-infamous dot.com days, entrepreneurs quickly gained access to the public markets. In Germany, this was true to a lesser extent for the technology sector around the turn of the millennium. Today, most start-ups will be in business for a number of years and complete several financing rounds before they can prepare to go public. A discussion about the various advantages and disadvantages of an IPO for the success of a start-up is beyond the scope of this Guide. We do want to mention, however, that the window for technology IPOs in Germany has not been particularly wide open over the last couple of years. Since 2015, only a few tech start-ups attempted an IPO in Germany, and results for investors were mixed. It remains to be seen if some of the (at least initially) more successful IPOs in 2017 and the batch of young tech company IPOs we have seen in 2018 so far will have a positive impact on the IPO environment in Germany and pave the way for other start-ups and their investors.

When considering a trade sale to a U.S. acquirer as an exit route, it must be noted that valuations are higher in the United States and many U.S. corporations have ample experience in acquiring emerging companies as part of their innovation portfolio, while start-up M&A is still not that common in the German market (though definitely on the rise). Operating through a U.S. company may ease each of these exit processes. Furthermore, certain favorable valuation methods such as the U.S.-style "forward or reverse triangular statutory merger" are not available for non-U.S. companies.

Access to Talent Pool and ESOPs: Finally, tapping into the rich talent pool of Silicon Valley and other U.S. tech hubs is easier for a U.S. legal entity as it can offer standard, market-tested equity-based employee participation plans with stock options (for details, see Chapter B.5 below).

WHICH U.S. COMPANY FORM TO CHOOSE

In most cases, it is advisable to incorporate NewCo in Delaware. U.S. companies are most commonly incorporated in Delaware because of the state's business-friendly reputation, which includes flexible business formation statutes (allowing flexibility in structuring business entities and allocating rights and duties), specialized, highly experienced courts dedicated to hearing corporation cases (which brings with it the additional benefit of well-established case precedent, which, in turn, provides greater guidance reducing the need for litigation) and an efficient Secretary of State (which reduces administrative burdens and hold-ups). Most U.S. investors also tend to prefer Delaware because of the ease with which capital stock can be transferred (including the ability to go public). Furthermore, the corporation law of Delaware enjoys the advantage of being widely familiar to legal practitioners across the United States.

In Delaware, it is common to establish one's company as a so-called "C Corporation." The corporation will then be taxed separately from its owners under U.S. federal income tax law. Its counterpart, the so-called "S Corporation," refers to a corporation whose shareholders are subject to income tax instead of the corporation itself, based on their *pro rata* shares of income. Every profit-oriented corporation will be automatically qualified as a C Corporation, whose shares do not need to be held by resident or citizen individuals or certain qualifying trusts, as it is the case for S Corporations. For a more detailed overview of the corporate (governance) structure of a Delaware Inc. see Chapter A.4.

Concerning which legal form to elect, sometimes the Limited Liability Company ("LLC") is discussed. However, although this newer, somewhat more flexible legal form is most akin to the German GmbH which German newcomers are familiar with, it is often not suitable for the purposes of German technology companies, *e.g.* U.S. investors often do not want LLC interests and while there are employee equity plans for LLCs, they are non-standard and will cost significantly more to create and maintain when compared to "standard" C Corporation equity plans.

DELAWARE INC. FEATURES IN A NUTSHELL:

Quick & Easy Incorporation — The incorporation of a Delaware Inc. happens quickly (within 1 day), underlies low formal requirements (possible per fax) and is low-cost (graded depending on the share capital).

Simple Decision Making Processes — The Delaware Inc. follows the "one tier" governance approach, *i.e.*there is only one operative and supervising board (board of directors). In addition, decision making is faster and simpler: mostly majority vote or written consent is required, rather than the super majority or unanimous consent.

Directors Liability — Directors' risks of being held liable for assessing the company's future business prospects when making financing decisions tend to be less strict in the U.S. than in Germany.

Corporate Capital — Statutory minimum capital requirements and strict capital maintenance rules, as they are characteristic for the German corporate law, do not exist for the Delaware Inc.

After incorporating in Delaware, the corporate entity will need to qualify to do business in the relevant federal states. This is easily done and cost effective. In order to minimize liability risks and facilitate a centralized administration and future transactions, it is strongly recommended to opt for a holding company as a TopCo with respective operating as well as sales and distributions subsidiaries. However, if such a structure should be too complex for the start-up at an early stage, this can be implemented later.

HOW TO DO A FLIP IN THREE STEPS

Here is a brief summary of the typical steps to be taken in a Flip. The best transaction structure will, however, always depend on the specific case at hand. Founders and investors of TechCo are well advised to bring an experienced counsel on board who can cover both the German and the U.S. tax and corporate law angles.

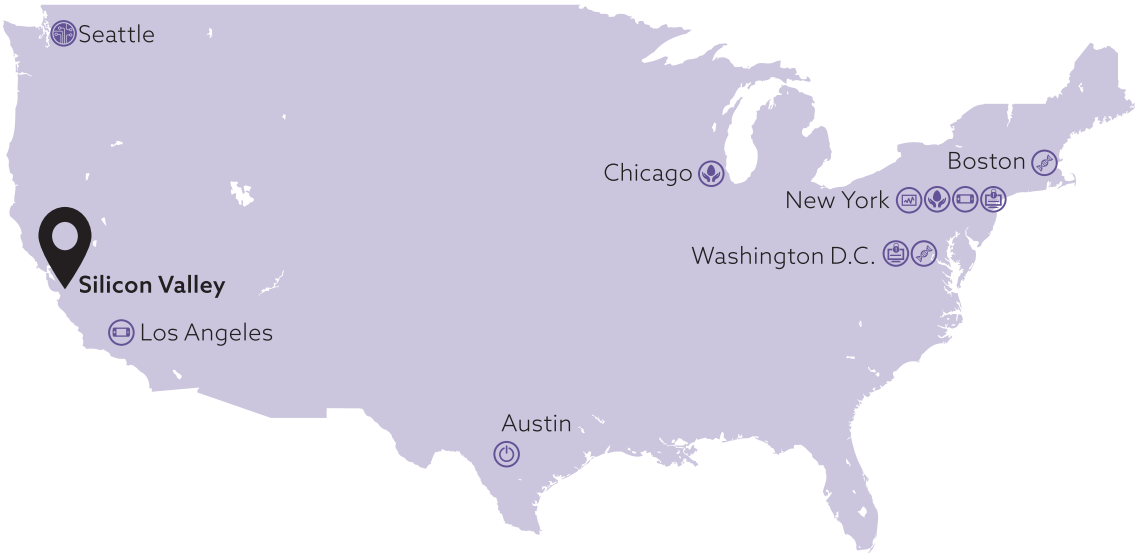
- **Step 1:** The current shareholders of TechCo incorporate NewCo.
- **Step 2:** The existing shareholders of TechCo transfer 100% of the shares in TechCo to NewCo. This will require a transfer deed to be notarized in front of a German notary. In exchange, the existing shareholders of TechCo receive shares in NewCo.
- **Step 3:** The current shareholders of NewCo and potentially the new investors enter into the typical agreements governing their rights and obligations as shareholders of NewCo, including exit options, preference rights etc. (for details, please see Chapter A.3 below).

A CLOSER LOOK:

LOCATION CONSIDERATIONS:

WHERE TO SET UP SHOP IN THE UNITED STATES?

When deciding where you are going to set up your place of business, take into account that some investors appreciate local proximity.
As Silicon Valley is a very expensive place to do business, with fierce competition for talent, be sure this is the right place for your business.
Some alternatives, depending on the main focus of business, are for example:



Biotech: Boston/Washington, D.C.

Insurance: New York/Chicago

FinTech/Ad Tech/Publishing: New York

Cybersecurity: Washington, D.C./New York

Hardware/Enterprise Software: Seattle

Other: Austin

Media/Games: Los Angeles/New York

CERTAIN TAX CONSIDERATIONS

The share swap underlying the Flip is a taxable (sales-like) event under German tax law. Unlike for share swaps involving EU/EEA companies, a Flip into a company organized under the laws of the United States cannot be effected on a "no gain/no loss" basis and there is no rollover of acquisition costs under the German Transformation of Companies Tax Act (*Umwandlungssteuergesetz*).

Thus, when implementing the Flip, the current shareholders of TechCo will record a gain (loss) at the balance of (i) the fair-market value (*gemeiner Wert*) of TechCo-shares and (ii) their carrying book value and transaction costs, each at the time of transfer of title (or if differing: economic ownership) in TechCo shares to NewCo.

For German income tax purposes, the determination of the fair-market value of shares in a non-listed company must primarily be derived from comparable sales in the same share class in the last year or, in their absence, from a commercially accepted valuation method.

With respect to the effective tax burden, the situation differs whether the respective shareholder of TechCo is a German corporation or a natural person subject to German taxation.

- For corporate shareholders, the regular German tax relief should often be available. Thus, 95% of any gain from the Flip would be tax exempt, with the remaining 5% increasing such corporate shareholder's taxable income. A loss would be fully tax exempt (no tax relief). Depending on the local trade tax multiplier, the 95% tax exemption leads to an effective taxation for a German corporate shareholder at approx. 1.5% of the gain from the Flip.
- In contrast to that, if the shareholder is a natural person subject to German taxation and holds an equity stake in TechCo of at least 1%, her gain from the Flip would only be 40% tax exempt, with effective taxation often ranging up to approx. 28.5%.

When contemplating a Flip, founders and investors should obtain advice from qualified tax lawyers both in Germany and the United States. For example, to avoid negative tax implications, it is important to demonstrate that NewCo is a "real" enterprise and not just a letterbox. NewCo should not become a "dual resident" from a tax perspective: Germany would treat NewCo as a German tax payer if it had a German central place of management, which may result in difficult double taxation situations. So the executive board of NewCo should be staffed in a way that the "center of gravity" for management of NewCo can be demonstrated to be in the United States. A clear distinction of management functions (in the United States) and shareholder supervisory functions (may be located in Germany) should be implemented to that end.

3. VC DEAL TERMS – UNITED STATES VS. GERMANY

More often than not, a U.S. venture capitalist and a German technology company agree on the commercial terms of an investment transaction and think that the hard work is done but quickly find themselves at an impasse over the way the transaction will be documented. With the increase in cross-border venture capital transactions, particularly U.S. investors taking stakes in German technology companies, this is an issue that companies and investors are dealing with more regularly than ever before.

KEY ELEMENTS OF A VENTURE CAPITAL TRANSACTION

A typical venture capital transaction, whether it is an investment into a U.S. or a German company, involves the following key elements:

- The investor purchases equity in a private company in return for cash.
- The company and, in some cases, its key executives or founders provide investment related protections (representations, warranties or indemnities) to the investors about the company and its business.
- The investor typically receives a class of preferred stock which provide for preference rights in case of a liquidity event and certain other rights, including rights to receive financial and other information relating to the company (for details see below).
- The investor is given board membership, granted board observer or other representation rights.
- The rights of the parties on an "exit," particularly an IPO or sale of the company, are defined.

From a commercial perspective, a venture capital transaction (where an investor or a group of investors privately acquire shares in a company) should essentially be the same transaction, regardless of jurisdiction. In practice however, documentation styles vary considerably outside the United States, which can be frustrating to many venture capitalists, the majority of which are U.S. based.

This chapter seeks to identify several of the more salient aspects in which typical U.S. and German financing round documentation diverge from each other. When comparing documentation used in typical U.S. and German venture capital transactions[3], a number of key differences emerge, including, in particular:

- Form and style of documentation (including the terminology used);
- Representations and warranties; and
- Scope and style of investor protections.

3 For a detailed overview of venture capital transactions in Germany see the new "Orrick's Guide to Venture Capital Deals in Germany" (available at: www.orrick.com/Insights/2018/02/Orrick-Guide-to-Venture-Capital-Deals-in-Germany-2018-Edition). This Guide discusses many of the most-contested issues in venture financings, presenting both the investor's and the founder's perspective. It gives an outline of venture deal structures in Germany, the industry terminology and some of the concepts and terms frequently used in term sheets and the fully fledged investment documentation in the German market.

TYPICAL VC-RELATED AGREEMENTS IN GERMANY AND THE UNITED STATES

German Financing Rounds: Investments in a German start-up (which are most often set up either as a "GmbH" or a "UG (haftungsbeschränkt)") are usually implemented through a share capital increase. In the course of such increase, new shares are created, which the investors subscribe for against payment of their nominal value. In addition, the investors will undertake to pay additional funds, *i.e.*, the bulk of the investment funds, into the company's capital reserves or to grant a (often convertible) shareholder loan to the company. As part of the financing round, all existing shareholders, the new investors and typically the company will enter into an investment agreement and a shareholders' agreement (sometimes the agreements are combined into one "investment and shareholders' agreement").

- In the investment agreement, the parties set forth the terms and conditions for the capital increase, the details for the additional funding (amounts, milestones etc.) and guarantees given by the company (and in many cases by the founders and to a lesser extent by existing investors) and the remedies in case of a breach.

- In the shareholders' agreement, the parties set forth their rights and obligations as shareholders of the company, including corporate governance aspects (managing directors, optional advisory board, appointment rights, etc.) and certain veto rights for the investors, transfer restrictions, drag-and tag-along rights as well as provisions regarding liquidity events and the distribution of the resulting proceeds, as well as anti-dilution protection.

In most cases, both agreements will need to be notarized. It should be noted that the management board of the German start-up cannot implement a financing round. Rather, the decision about a financing round rests with shareholders as the capital increase requires a shareholders' resolution be adopted by at least 75% of the votes cast. For practical purposes, in many cases de facto, the consent and active support by all shareholders is required or at least very advisable.

U.S. Financing Rounds: It should be noted that unlike in the German market, where standards for venture financing transactions are only slowly developing, well established market standards exist in the United States, which helps in simplifying the implementation of financing rounds following the investors' positive funding decision.

U.S. financing rounds usually include the following agreements:

- The new investors and the company will enter into a stock purchase agreement under which the new investors will typically purchase preferred stock (please see below for a summary of customary preference rights in U.S. transactions). This stock purchase agreement will contain certain representations and warranties given by the company, including regarding the validity of the preferred stock being purchased and in most cases certain operational and financial representations and warranties.

- The company's charter (also referred to as certificate of incorporation), together with its bylaws, will set out certain rights of the shareholders, including liquidation preferences, anti-dilution protection and veto rights (for details see below).

- In an investors' rights agreement, the investors are granted certain rights, which typically includes information rights, pre-emptive rights in case of future issuance of new securities and registration rights pursuant to which the investor can request

the company to publicly register the company's common stock with the U.S. Stock Exchange Commission (SEC) in connection with or following an IPO of the company.

- In a separate voting agreement, the parties stipulate how the stockholders will appoint and remove directors on the company's board. These agreements may also contain provisions regarding the shareholders' obligations to vote in favor of exit transactions (known as a "drag along"), provided that certain criteria are fulfilled (*e.g.*, approval of the transaction by the board, a majority of common stock and a majority of preferred stock).
- Finally, the parties may enter into a separate right of first refusal and/or co-sale right agreement, which states that if holders of common stock propose to sell their shares to a third party buyer, the holders of preferred stock have a right of first refusal to match the third-party offer or alternatively the holders of preferred stock can participate in the sale ("co-sale") by selling their preferred stock on a *pro rata* basis.

Please note that the above list is just a high-level summary and that these agreements can vary across transactions and sometimes the agreements are combined.

REPRESENTATIONS AND WARRANTIES IN VC DEALS

While U.S. companies will usually give representations and warranties in the transaction documentation, the investment agreement in a German financing round will include guarantees within the meaning of Section 311 German Civil Code that provide for a liability irrespective of fault. It should be noted, however, that in practice the difference is mainly in terminology.

Where German and U.S. investment agreements differ is the manner in which disclosures (or exceptions) to the warranties are given. While the form of delivery of "specific" disclosures does not differ too much (in the United States and Germany, one usually finds a schedule of exceptions or disclosure schedule, while for example in U.K. investment rounds, a disclosure letter is the more frequent form), it is the additional inclusion of "general" disclosures in Germany that is the material difference. General disclosures are typically disclosures of those matters of which the investor is deemed to have public knowledge, such as matters on public record and frequently the entire data room (or at least a large bundle of specific documents) being deemed disclosed (though, in Germany generally no disclosure against "core guarantees" such as title and freedom of third-party rights with respect to shares, is accepted). General disclosures, however, are not a usual feature in the U.S. transactional landscape and as such, by and large, they are met with resistance by U.S. investors.

In Germany, a number of limitations are given on the liability of the representations and warranties, such as time limits within which claims must be made, caps on liability of the warrantors and minimum financial levels for claims before they can be made. These limitations are frequently the subject of detailed negotiation between the parties. While these types of provisions are common in U.S. mergers and acquisitions and private equity transactions, they are far less common in U.S. venture financing transactions. In the United States, most venture financing transactions do not have a time limit (other than applicable statute of limitations), caps on liability or minimum financials levels for claims.

Indeed, in the U.S., there is typically not a provision in the agreement that details how investors would even bring a claim against the company.

Finally, in the United States, founders do not typically make representations or warranties as individuals. However, in Germany, at least, business guarantees are often given by founders, with their liability capped at a 2-3 multiple of annual salary in the current market environment.

One area of common ground between representations and warranties, given in typical U.S. and German venture capital transactions, is that it is rather unusual for actual claims to be made. The threat of litigation is nonetheless seen as a valuable way of ensuring thorough disclosure and of driving an investor's due diligence investigation of a company.

TYPICAL PREFERENCE RIGHTS AND PROTECTIVE COVENANTS IN VC FINANCINGS IN THE UNITED STATES AND GERMANY

Below are some of the preference rights and protective covenants one typically finds in the U.S. and the German venture capital market. Of course, the use of such investor-favorable deal terms depends, inter alia, on the current market environment and how "hot" the respective company is and how many investors are competing to get the deal. Overall, we noticed in recent quarters a slight shift to more investor-favorable deal terms, with the U.S. venture environment remaining below peak levels of the past few years, although venture capital sentiment is still well above historic averages.

- **Liquidation Preference:** Shares of preferred stock will generally be entitled to receive liquidation preference prior to any payment of proceeds to holders of common stock upon a change of control or other liquidity event. This downside protection is an amount generally equal to 1x the amount invested, although it could be higher, which is paid in preference to other series of stock. While in some cases the liquidation preference is "participating" or "capped participating," the most common structure in U.S. venture transactions is 1x, non-participating. According to our experiences, German transactions generally show similar liquidation preferences, in many cases investors receive a 1x non-participating liquidation preference (einmalige, anrechenbare Liquidationspräferenz).

- **Conversion Rights:** Shares of preferred stock are generally convertible into shares of common stock on a 1:1 ratio. In the event of a change of control or other liquidity event, the holders of preferred stock have a right to convert to common stock and will generally elect to do so if it results in them receiving a greater portion of the proceeds from such transaction. The preferred stock will usually convert automatically upon an IPO of the equity securities of the company.

- **Anti-Dilution Rights:** Anti-dilution protection has long been a standard feature of both U.S. and German venture capital transactions. Within the United States, almost all transactions use a broad based weighted average formula for calculating anti-dilution. That said, certain later stage transactions (*i.e.*, 12-18 months pre-IPO) and companies raising capital from more traditional private equity funds (rather than venture funds) in the U.S. will sometimes include a ratchet or narrow-based weighted

average protection. In the German market, we have recently seen most anti-dilution protections to be modeled as a narrow-based weighted average, though full-ratchet covenants are still seen more often in sectors where investment funds are particularly scarce, *e.g.*, in the life science sector.

The main difference between anti-dilution rights in the United States and Germany is not so much the way in which the adjustment is calculated but rather the manner in which any anti-dilution benefit is provided to the existing shareholders. In Germany, upon the occurrence of an anti-dilution event, the usual practice is to obligate all shareholders to vote in favor of a capital increase and grant the investor entitled to the anti-dilution protection such number of shares to compensate for the requisite dilution. In the U.S., due to the potential impact of deemed dividend rules (*i.e.*, the granting of additional shares being seen by the IRS as deemed dividends), additional shares are not granted and instead there is an adjustment to the conversion rate of the preferred stock to common stock, such that the investor does not hold additional stock today but does hold and control a greater percentage of the company on an as-converted basis.

- **Voting Rights:** Preferred stock generally has the right to vote on a number of items, including specific preferred directors on the board and to approve certain material corporate transactions. Such protective provisions would prohibit the company from taking such action without the consent of a certain percentage of the preferred stock. Such matters typically include liquidation of the company, effecting a sale of all or substantially all of the company's assets, redemption of shares, assumption of debts or creation of debt securities beyond certain amounts or ratios, changes to the company's employee stock option program ("ESOP"), etc. In addition, some companies will permit board members elected by the holders of preferred stock to have veto rights or special votes with respect to management and operational decisions.

  Based on our experience, U.S. investors – particularly those on the West Coast – tend to request fewer veto rights when it comes to management and day-to-day operational decisions, opting instead to grant more freedom to the founders in order not to stifle the agility of the company. Investors in the German market often tend to require more control than their U.S. peers.

- **Pro rata or Pre-Emptive Rights:** Typically, holders of preferred stock will have the right to purchase a *pro rata* portion of any new issuance of equity securities or convertible debt securities of the company. Similar provisions are also found in the German venture capital landscape. Please note, however, that German law requires new issuances of shares to be first offered pro-rata to the existing shareholders unless otherwise waived by the shareholders either in relation to the specific case at hand or generally.

- **Right of First Refusal and Co-Sale:** These preferences provide the rights of holders of preferred stock to a right of first refusal with respect to any sale of common stock by certain key holders of common stock of the company (typically any holder of 1% or more of the company's common stock). In the United States, the company will typically have a primary right of first refusal on all sales of common stock, while the holders of preferred stock will have a secondary right of first refusal if the company declines to exercise its right of

first refusal. In addition, such holders of preferred stock are granted co-sale or tag-along rights with respect to transactions where the right of first refusal is not fully exercised. In German market transactions, tag-along rights are frequently granted to every shareholder (*i.e.*, not only preferred shareholders) and rights of first refusal or pre-emption rights apply in the case of a transfer of common stock or preferred stock. In both the United States and Germany, there are customary carve-outs, including for transfers to affiliates.

- **Information Rights:** Generally, the investors' rights agreement will provide that certain large investors (often referred to as "Major Investors") will be entitled to receive financial statements and annual budgets from the company and will have the right to inspect the property of the company at reasonable times. According to our experience, in German financing rounds the investors' information rights tend to be broader and apply to all shareholders irrespective of the size of their holdings. Please also keep in mind that under mandatory German law the holders of shares in a German GmbH have unalienable information rights even if they only hold one share. Similarly, stockholders in Delaware corporations have statutory information rights, so certain U.S. companies will include a "statutory information rights waiver" in the stock purchase agreement, whereby the non-Major Investors waive their information rights.

- **Registration Rights:** Holders of preferred stock generally have the right to force a company to file a registration statement with respect to their shares, even if the company has not already gone public, typically within five years following their investment. Similarly, such holders will have the right to piggyback on other registration statements filed by the company, subject to certain exceptions, including public filings relating to ESOPs. In our experience some companies backed by U.S. investors have been able to exclude an IPO from the registration rights requirements (meaning only piggyback or S-3 registration would be able to be forced by the holders of preferred stock). In practice, registration rights are rarely if ever exercised by U.S. investors other than in connection with the company's IPO.

  By contrast, in any listing of a company's shares on a German exchange or another European market, the entire issued share capital of the company is included. Consequently, registration rights are not relevant when seeking a listing outside of the United States.

- **Drag-Along Rights:** In the voting agreement, the stockholders often agree that in the event a minimum number of shareholders (and the Board if applicable) approve a liquidity event, all other shareholders are forced to vote their shares in favor of the transaction. The threshold vote usually requires the vote of a majority of the preferred stock as well as either a majority of the common stock or a majority of all capital stock. The vote sometimes includes separate votes of individual series of preferred stock, particularly where different series invested at varying valuations and may have different economic incentives. Here, a balance needs to be found between the interests of the company and the founders, which is to ensure that stockholders will vote in favor of a company sale (since acquirers will often require that 90%-95% vote in favor),

and the interests of investors who will often want a separate vote in order to protect their economics. In practice, companies sometimes agree to a series vote but structure that series vote as one that goes away once the multiple of the return for an investor on a transaction reaches a certain multiple, *e.g.* 2x-3x. In the German market, we usually see drag-along rights that are triggered if shareholders holding together more than 50% of the entire nominal capital of the company request an exit. In addition, often an investor majority (and sometimes even a majority of each class of preferred shares) is required.

A CLOSER LOOK:

SOME RECENT DEVELOPMENTS IN U.S. VC SEEN IN TERM SHEETS

HERE ARE SOME FURTHER RECENT DEVELOPMENTS THAT WE HAVE SEEN IN TERMS SHEETS WITH U.S.-BASED INVESTORS:

Anti-Sexual Harassment & Diversity: Lately, we have seen VC investors in the U.S. pay closer attention in their investment decisions to how companies handle the issues of sexual harassment, discrimination and lack of diversity. Although this is still an ongoing development, we have also come across term sheets with covenants requiring the target company to adopt anti-harassment and anti-discrimination policies within a short period after closing and to ensure that all employees are well informed and aware of such policies. Other investors have announced zero tolerance policies and conducted comprehensive investigations of any allegation of misconduct in any of their portfolio companies. For more information please refer to p. 48 *et seq*.

ICO Protection: Some U.S. investors have added language to their standard term sheets barring ICO's or token offerings without either board approval that includes the preferred directors or approval of a majority of outstanding preferred stock. According to our experiences, the VC community in general has not included *pro rata* rights relating to token offerings, though we have seen a few instances where a VC investor has taken the position that its *pro rata* rights apply to token offerings and many are starting to seriously consider it. Some are of the view that asking for a *pro rata* on token offerings isn't entirely fair as it's akin to asking for a cut of the Company's revenue. Others believe it's a reasonable ask since a company that pursues token offerings may only do one or two equity financing rounds. As the blockchain/crypto movement continues to grow, we expect the VC community to adjust accordingly.

4. THE DELAWARE INC. – CORPORATE GOVERNANCE BASICS

Delaware is the preferred jurisdiction in the U.S. for venture financing by U.S. investors and IPOs listed in the U.S. on Nasdaq or NYSE. It is also the preferred jurisdiction to enable an acquisition through a merger transaction, which is the preferred transaction structure for U.S. buyers due to merger statutes in the United States. This Chapter gives a brief overview of the applicable rules governing a Delaware Inc., more precisely a C-Corporation.

COMPANY CONSTITUTION

Delaware corporations are governed by the Delaware General Corporation Law ("DGCL").

The basic constitutional documents relevant for a corporation are the certificate of incorporation, which establishes the formation of the corporation upon filing with the Secretary of State of the State in which the corporation is incorporated, and the bylaws, which set forth the fundamental rules and procedures by which the corporation will be governed. As promptly as practicable after incorporation, the incorporator would typically elect the initial board of directors, who would then hold their first organizational meeting, in which shares of stock are approved to be sold, officers are appointed, and other initial actions are authorized.

The certificate of incorporation must include:

- The name of the company;
- The address of the company's registered business office in Delaware and the name of its registered agent;
- The nature of the business purposes to be conducted or promoted; and
- In the case of corporations, information about the company's securities (stock or membership interests).

Though not mandatory, the following provisions are frequently found in certificates of incorporation:

- The right of directors to amend or repeal company bylaws or the limited liability company agreement;

- Director protections, including limitations on personal liability under certain circumstances; and
- Any limitations on the term of the company's existence.

The bylaws can contain any provision, not inconsistent with law or with the certificate of incorporation or formation, relating to:

- The business of the company;
- The conduct of the company's affairs; and
- The company's rights or powers or the rights or powers of its stockholders or members, directors or managers, and officers or employees.

The bylaws typically specify how the company is managed, the conduct and frequency of meetings, indemnification of directors or managers, etc. The bylaws may be adopted, amended, or repealed by the stockholders entitled to vote or if the certificate of incorporation permits, the board of directors.

Stockholders of a Delaware Inc. may also enter into stockholder agreements that provide for rights beyond those set out in the DGCL or in the entity's organizational documents mentioned above. For an overview of such stockholders' agreements that are common in VC-backed companies please see under Chapter A.3 above.

GOVERNANCE – OVERVIEW

In its purest sense, the U.S. American corporate governance structure is pyramidal in form. Stockholders occupy the base and are empowered to vote on major corporate actions and to elect members to sit on the board of directors. The next tier aligns to the board of directors, whose role is to develop corporate strategy and policy and to advise on management decisions. At the apex is the band of corporate officers and their inferior agents or employees. Generally, the corporate officers and agents are the individuals who run the day-to-day business operations.

American corporate governance structure is rooted in the separation of ownership and control. While a corporation is typically owned by multiple stockholders, these stockholders likely lack sufficient knowledge and incentive to participate in the daily management of the business given their (often) small stake in the corporation. Therefore, it is more efficient to delegate management responsibilities to a small number of experienced professionals whose sole focus is to grow the business.

Unlike the two-tier corporate governance model used by jurisdictions outside the United States, the single board corporate governance scheme adopted by the DGCL allocates primary control of the corporation to either one or multiple individuals who are collectively called a "board of directors." Legally required to act in the best interests of the stockholders, the board of directors supervises the corporation's business and affairs and is responsible for hiring corporate officers to manage day-to-day business operations.

BOARD OF DIRECTORS

Every corporation must have a board of directors. The board of directors represents stockholders and its members are elected by stockholders to oversee the corporation's management and business strategies. The board of directors has two main functions: decision-making and oversight. The decision-making function involves evaluating and approving strategic goals, selecting and advising officers and senior management, approving capital raising activities, and acquiring or disposing of material assets. The directors' oversight function involves monitoring the corporation's financial performance, personnel performance, and ensuring the corporation has adequate policies to comply with applicable legal obligations and internal bylaws.

The consent of the board of directors will generally need to be obtained for:

- Appointment of officers;
- Material agreements such as leases, strategic partnership agreements, incurrence of indebtedness, guarantees of indebtedness, material license agreements and other agreements governing major transactions;
- Approval of and recommendation to the stockholders to adopt amendments to the certificate of incorporation;
- Approval of and recommendation to the stockholders to enter into fundamental transactions, such as a sale of the company or merger;
- Approval of stock options;
- Approval of annual budgets; and
- Evaluation of compensation for major executives.

In addition to the foregoing general restrictions, holders of preferred stock may request certain decisions of the board of directors to be made only with the consent of specific directors appointed by a particular series of preferred stock. Such provisions could also be found in the investors' rights agreement (as described above, please see Chapter A.3). Examples hereof are:

- Any capital expenditures over a certain material threshold;
- Entering new lines of business or discontinue current lines of business;
- Hiring, firing or changing the compensation of CEOs;
- Making investments conflicting with investment policies; and
- Making advanced payments to any person.

The board has one or more directors. Unlike in Germany, U.S. law does not provide for statutory rights of employees to board representation.

There are no general restrictions or requirements for the appointment of directors, except that they must be natural persons. There is no statutory requirement that:

- a director must be a stockholder or reside in the United States; or
- a number of directors must be U.S. citizens or permanent residents.

However, having a majority of board members residing outside the United States or having the board of directors regularly making decisions outside the United States can have potentially adverse tax consequences. For example, Germany would subject a U.S. corporation to German taxation if it had a German central place of management,

which may result in difficult double taxation situations. It is thus important to demonstrate the "center of gravity" for management decisions is in the United States.

A clear distinction of management functions (in the United States) and stockholder supervisory functions (may be located in Germany) should be implemented to that end.

CORPORATE OFFICERS

A corporation operates through its agents, and officers are the principal agents of a corporation. Corporate officers receive their grant of authority from the board of directors. Because Delaware is home to many businesses of varying sizes – each with its own products, services, and business models – the DGCL provision governing corporate officers aims to serve as a one-size-fits-all rule that applies to all corporations. Consequently, the exact scope of authority of an officer relative to that of a director is not easily defined.

Section 142 DGCL, however, specifies that officers' titles, responsibilities, and compensation are to be determined by the bylaws of the corporation enacted by the board of directors. Thus we recommend that either the bylaws of the corporation or the board of director resolutions appointing officers delineate the authority and powers of the appointed officers. Typically, officers are the only representatives of a corporation that have authority to execute contracts and enter into binding arrangements on behalf of a corporation, unless other individuals are granted such authority by the board.

The statutory minimum number of corporate officers is two. The DGCL at one time suggested that a corporation have at least a President and a Secretary ("Chief Executive Officer," "Chief Financial Officer" and similar titles were historically fictional in nature, but the DGCL currently recognizes these titles as official officer titles for corporations), but there is currently no specific requirement for which officer positions a corporation must have, nor is there a statutory maximum number of officers.

The appointment of corporate officers is entirely at the discretion of the board of directors. Like directors, the only qualification is that it be an individual person. The same individual can be appointed to multiple officer positions, and there is no statutory prohibition against corporate officers also serving on the board of directors. It is common for one or several senior officers to sit on the board and serve as the nexus between the daily company operations and the high-level decision making conducted by the board.

A few words regarding the roles of "President" and "CEO": The top management function is vested by the board in the President or CEO. As noted above, the DGCL previously formally recognized only the role of "President," and "CEO" was a fictional title that had no actual authority. However, with the proliferation of the usage of "CEO" among U.S. corporations, the DGCL currently does not specify any particular officer title. Although some corporations appoint two separate individuals to serve as President and CEO (and there is no clear guidance as to which position would have greater authority), most corporations, in particular closely held corporations, have one person serving in both capacities (or, more frequently, just the CEO, which is also acceptable). The CEO reports directly to the board of directors and is responsible for executing the strategies set in place by the board and for overseeing the management and performance of all corporate agents. In closely held corporations, the CEO often also serves on the board of directors, sometimes serving as chairman.

FIDUCIARY DUTIES AND LIABILITY RISKS

Delaware common law maintains that directors, officers and, in certain instances, controlling stockholders owe fiduciary duties of care and loyalty to the corporation they serve and its stockholders. These duties comprise:

- **Duty of Care:** Directors of a Delaware corporation have a duty to act with the "amount of care which ordinarily careful and prudent men would use in similar circumstances." While directors have no per se duty to maximize the profits of the corporation, directors must exercise the requisite degree of due care to protect the financial interests of the organization and its stockholders. Therefore, it is the director's obligation to inform themselves "prior to making a business decision, of all material information reasonably available to them."

- **Duty of Loyalty:** As the elected representatives of the stockholders, who are the true owners of the corporation but largely powerless with respect to the corporation's strategy and management, the duty of loyalty fulfills the directors' and officers' obligations to act in the best interests of the corporation and its stockholders. The duty of loyalty intends to protect the corporation from a director or officer "us[ing] their position of trust and confidence to further their private interests."

- **Duty of "Good Faith":** Over the last decade, Delaware courts have debated whether the duty to act in good faith is an independent fiduciary duty or a component of the duties of care and loyalty. The most recent jurisprudence on the matter distinguished the "concept of good faith from the duty of care and duty of loyalty" and established good faith as an element of the duty of loyalty. The Supreme Court of Delaware has not explicitly defined good faith, and instead chose to outline two categories of behavior constituting bad faith. The first category includes "fiduciary conduct motivated by an actual intent to do harm." Under the second category, bad faith is established when "the fiduciary intentionally acts with a purpose other than that of advancing the best interests of the corporation, where the fiduciary acts with the intent to violate applicable positive law, or where the fiduciary fails to act in the face of a known duty to act, demonstrating a conscious disregard for his duties." The latter category may be applicable in circumstances where a director's actions are more culpable than gross negligence without a traditional self-interest conflict.

- **Duty of Oversight:** Directors have a duty to exercise care in overseeing that these officers are properly executing their assigned tasks. This duty of oversight derives from the duties of care and loyalty, but is not recognized by Delaware courts as a fiduciary duty on its own. The Delaware Supreme Court has held that a director breaches his duty of oversight when he has "utterly failed to implement any reporting or information system or controls [or] ... having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."

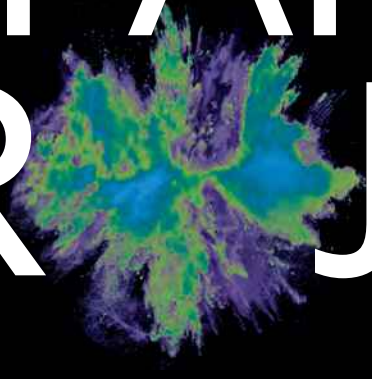
- **Duty of Disclosure:** Like the duty of oversight, the duty of disclosure is not an independent fiduciary duty but a subset of the duties of care and loyalty. Under Delaware common law, directors have a fiduciary duty to "disclose all material information to stockholders when seeking stockholder action."

A breach of any of the directors' or officers' fiduciary duties would enable the stockholders of the corporation (or any of them) to bring a claim against the director or officer personally. Against the wide scope of these duties (that keep being developed and fine-tuned by the courts) U.S. case law has established the business judgement rule as a safe harbor for directors and officers to prevent inertia for fear of liability risks. Under this rule, a director's action is deemed valid if the director has acted on a basis of information, in good faith, and in the true belief that her action was in the company's best interest. Delaware corporate law further stipulates that directors can rely in good faith on information, opinions, reports or statements from officers, employees, board committees' members, or any other person (also outside the company's organization) regarding matters the director reasonably believes are within that person's professional or expert competence, provided that the person has been selected with reasonable care by or on behalf of the company.

Under certain circumstances, directors can eliminate/limit their liability for breaches of fiduciary duties, and directors and officers can both enter into indemnification agreements with the corporation, pursuant to which the corporation will defend, at the cost of the insurance company, relevant directors and officers against incoming claims.

B.

U.S. EXPANSION PROJECTS



1. HOW TO USE AND PROTECT A TRADEMARK IN THE UNITED STATES

Often, a German technology company's brand is one of its most valuable assets. By properly registering and using the company's trademark, it can make sure that its brand is fully protected as the company enters the U.S. marketplace.

TWO WAYS OF OBTAINING TRADEMARK PROTECTION IN THE UNITED STATES

In the United States, like in Germany, it is somewhat unique that one can obtain limited protection for a trademark without first filing a trademark application. A company can obtain common law trademark rights – at least with respect to the geographical area that company is operating in – just by using its mark in connection with its product or service and providing it in commerce. Thus, by just using a trademark in commerce in the United States, a company will begin to accrue some rights to the mark (for more see below).

Obtaining a federal trademark registration from the United States Patent and Trademark Office ("USPTO"), however, confers certain important rights and legal benefits, including a legal presumption that the trademark is valid. A federal registration also serves to put others on notice of the company's use of the trademark. As a registered trademark will appear in the USPTO's database, it may also help ward off potential infringers from adopting a confusingly similar trademark.

OBTAINING A FEDERAL REGISTRATION

To obtain a federal registration for a trademark in the United States, an application must be submitted to the USPTO along with the government filing fees, which are currently USD 275 per class. The USPTO will register many different types of marks, including word marks, logo marks, and slogans, as well as trademarks that consist of trade dress or product packaging. The trademark application will need to include a clear drawing of the specific trademark being registered, such as the specific words typed out or an image file of your logo. The application will also need to include a clear description of the goods and services for which the mark is used, along with the correct classification number for these goods and services. The USPTO maintains a searchable database of acceptable

descriptions for goods and services located at www.tmidm.uptos.gov/id-master-list-public.html. The application will also need to include accurate ownership information for the owner of the trademark, including the entity name, address, entity type and country or state of citizenship.

Finally, the application will need to specify on what basis the applicant is seeking registration for the trademark. The two most common filing bases are either that the trademark is currently in use in interstate commerce in the United States – known as a 1(a) basis – or that the trademark is intended to be in use in the near future in interstate commerce in the United States – known as a 1(b) basis. An application filed on an in use basis will need to include specimens showing the mark being used in connection with a product or service being offered for sale, along with the dates on which the trademark was first used. An application filed on an intent to use basis will not need to include this information, however, the applicant will need to later file either an Amendment to Allege Use or a Statement of Use submitting specimens and dates of first use before the trademark can actually register.

There are, however, two additional filing bases for submitting a trademark application in the United States, both of which may be more attractive for a company based outside of the United States to utilize. One such additional basis relies on an existing, valid registration in the applicant's country of origin for the same mark being applied for in the United States. This basis is referred to as a 44I filing basis. To complete an application on this filing basis the applicant will only need to provide the USPTO with a true copy of the existing registration for the mark, along with a verified statement that the applicant has a bona fide intent to use the mark in commerce in the United States. A fourth filing basis involves the extension of an international registration for a mark filed through the World Intellectual Property Organization (WIPO) into the United States. This basis is referred to as a 66(a) filing basis. Both of these filing bases do not require specimens of use to be submitted to the USPTO in order for the mark to get registered, which in some cases make these filing bases more attractive for German technology companies coming to the United States.

The application process typically takes about a year to complete, with the application first reviewed by an examining attorney about three months after being filed. If the examining attorney finds any issues with the application, she will issue an Office Action, and a response will be due six months later. Once an application is reviewed by an examining attorney and found acceptable, it will be published in the Official Gazette of the Trademark Office. Subsequently third parties may file a formal opposition against your application if they believe the application is in violation of their rights. If an application does not receive an Opposition (or after an Opposition is successfully defended against), the USPTO will then issue a registration certificate if the application was filed based on use (1(a)), based on a foreign registration (44I) or based on a WIPO application (66(a)); if the application was based on an intent to use (1(b)), then a Notice of Allowance will be issued. For applications that receive a Notice of Allowance, the owner will be given six months to either file a Statement of Use or an extension request. The mark will need to be in use in the United States within three years after the Notice of Allowance is issued.

Once granted, a registration will remain valid as long as the mark continues to be used and the registration is renewed. The applicant will need to file documents with the USPTO attesting to continued use of the mark before the sixth anniversary and then again before the tenth anniversary of the registration date. After that, the mark will need to be renewed every ten years.

HOW TO USE AND PROTECT TRADEMARK IN THE U.S. WITHOUT A REGISTRATION

Many companies are interested in protecting their brands but are sometimes unclear about how to protect a trademark and, most importantly, how to use it properly. As mentioned above, trademarks do not have to be registered with the USPTO in order for the owner to have rights. However, it is advisable to file a trademark application with the USPTO in order to obtain a higher level of protection and certain benefits.

Although the circle R symbol ® cannot be used until the trademark is registered with the USPTO, the company can use a TM or SM superscript to indicate that it is claiming common-law rights in its mark. When the company is using a trademark in its advertising material or on its website, it should consider using the TM or SM superscript in the upper right-hand corner of the mark.

We advise using the TM or SM superscript in the first or most prominent use of the mark on the web page or collateral. In other words, the first time the trademark appears in the collateral, advertisement or web page. It is not necessary to use it every time, but the most prominent usage will put viewers or readers on notice that the company is claiming common-law rights to that mark. The TM or SM superscript can be a great deterrent to other individuals or entities who are considering the same or similar mark for their product or services.

It is also important to highlight the trademark in some way to set it apart from the rest of the company's advertising language. It is not necessary to capitalize the trademark, but it is a good idea to highlight it in some way to pull it out from general text, either through bold, underline, italics or a different font or stylization.

Another common mistake many make is to use a trademark as a noun or a verb. It should be ensured that the trademark is only used as an adjective, not as a noun or verb, or as a plural or possessive. For example, "Our ORRICK legal services support start-up companies who are looking to...."

2. INTERNATIONAL DATA TRANSFER WITH THE UNITED STATES

The transfer of personal data such as employee or customer data, from the EU to the United States has become a hot topic for many companies, not only for legal but also for business reasons. In particular, the outsourcing of data processing services to U.S. vendors should thus be carefully considered and planned.

GENERAL REQUIREMENTS FOR DATA TRANSFERS – THE EU/U.S. PRIVACY SHIELD

Under the new EU Data Protection Regulation ("GDPR") – which threatens with fines of up to 4% of global turnover and easy damage claims before courts – and the new German Federal Data Protection Act ("BDSG") any transfer of personal data must pass a two-step test: (i) would the data transfer to another legal entity be permissible if it was to take place within the EU/European Economic Area ("EEA"), and (ii) is the country to which data shall be transferred approved as providing for an adequate data protection standard, or are other appropriate means to protect the data in place? In addition, the GDPR provides for extensive notification requirements which may pose a significant burden as it may compromise the confidentiality of transactions.

PASSING THE FIRST STEP

As with any data transfer to another entity within the EEA, any data transfer to third parties or affiliates outside the EEA must be justifiable. When engaging an entity with performing certain data processing operations, for example, providing centralized hosting services or for performing direct marketing activities such as calls or emailing, such service providers often qualify as a data processor. If so, the data transferring and the data receiving (processing) entity must enter into a data processor agreement, which must meet all requirements of Art. 28 GDPR. Companies should review carefully whether a proposed data processing agreement meets these requirements, as they are fairly burdensome. However, both a missing agreement and an agreement that is not fully compliant can trigger substantial fines. In the case of data transfers to other entities that do not qualify as a data processor, one needs to check whether the transfer is permissible based on consent of the data subjects, the requirements for the performance of

a contract or otherwise permissible based on a balancing of interest test. Please be aware that European supervisory authorities tend to apply strict scrutiny when assessing whether a data transfer is permissible. Even though under the GDPR, data transfers to other group affiliates are facilitated, a free flow of personal data between group entities is not permissible. Each data transfer must serve a specific legitimate interest and there must not be any contradicting prevailing interests of the data subjects. In particular, the extensive notification requirements under the GDPR which require the transferring as well as the data receiving entity to inform of the data transfer, the purposes and various other specifics all outlined in Art. 13 and 14 GDPR, often require companies to rethink their strategy and to omit the transfer of personal data in general. Meeting these obligations should be considered early-on and where possible, one should consider sending anonymized data only.

PASSING THE SECOND STEP – EU/U.S. PRIVACY SHIELD OR STANDARD CONTRACTUAL CLAUSES?

With the recent public discussion around the fall of the EU/U.S. Safe Harbor Program in 2015, it became widely known that the United States is generally not approved as providing for an adequate data protection standard in terms of EU data privacy laws. In 2016, the EU Commission and the U.S. Department of Commerce quickly found a successor to the EU/U.S. Safe Harbor Program which is now called the EU/U.S. Privacy Shield (see: www.privacyshield.gov/welcome).

Companies transferring personal data to the United States have various options for passing the second step:

- **EU/U.S. Privacy Shield:** If a U.S. company has signed up for the program with the U.S. Department of Commerce, it is deemed as being located in a country that is approved as providing an adequate data protection standard. As a result, the transfer of personal data to such a company, for example, a new U.S. affiliate or vendor, only has to meet the requirements for intra-EU data transfers (see requirements of the first step above). However, the U.S. company must adhere to certain principles on the processing of personal data as specified by the EU/U.S. Privacy Shield, and any breach can lead to significant enforcement actions by U.S. regulatory bodies and to the suspension of data transfers from the EU. In practice, it is often favorable to rely on the EU/U.S. Privacy Shield if data is transferred to a longer chain of various data processors. Investors should be aware that the EU/U.S. Privacy Shield is currently legally and politically challenged. It may well be that the shield will soon be either modified or declared void by the European Court of Justice.

- **Standard Contractual Clauses:** Another option to meet the second step as outlined above is to enter into the so-called Standard Contractual Clauses (also called Model Clauses) as approved by the EU Commission (http://ec.europa.eu/justice/ data-protection/international-transfers/ transfer/index_en.htm). Once both the data exporting as well as the data importing entity have signed the appropriate Standard Contractual Clauses, any data transferred to the United States is deemed as being protected by appropriate contractual safeguards. The advantage of these Standard Contractual Clauses is that they are standard and must not be modified. This generally facilitates the negotiations with the U.S. counterpart. However, in order to meet the first step, the company must ensure that the Standard Contractual Clauses are amended so that they meet, for example, the requirements of Art. 28 GDPR.

IMPLICATIONS FOR DATA TRANSFERS TO A U.S. AFFILIATE

As mentioned before, German data privacy law and the new GDPR do not permit a free flow of data between affiliated companies. German companies should thus carefully consider which data it needs in the United States and then, based on that consideration, enter into the appropriate data transfer/processing agreement in order to ensure that both steps of the two-step tests are passed. For such intragroup data transfers, the Standard Contractual Clauses are most often the best option to work with.

USING U.S. SERVICE PROVIDERS AND DATA TRANSFERS

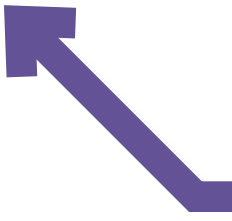
Even though many U.S. service providers, in particular, cloud services providers, offer attractive services for competitive prices, the engagement of such a service provider with data centers in the United States should be carefully planned.

As outlined above, any German technology company that wants to engage such service providers with the processing of EU personal data must enter into fairly complex data processing agreements. In addition, German supervisory authorities often require more than what is the generally accepted standard in the EU (see Orientierungshilfe Cloud Computing at www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf or the BSI Cloud Computing Compliance Controls Catalogue C5) which are fairly onerous and may thus (at least initially) not be accepted by U.S. providers.

Further, if German or U.S. entities provide services to EU customers, the data processing agreements entered into with the EU customers need to be carefully drafted as most of their obligations need to be passed down to the U.S. providers who are often reluctant to agree to agreements that deviate from their own standard data processing agreements. It is thus imperative to first conduct a careful review of the U.S. providers' data processing agreements and their security standards for compliance with EU and other internationally accepted standards before any commercial decision is made. In our experience, the willingness of adjusting data processing agreements to EU customer needs significantly decreases once the main master services agreement is signed. In addition, one needs to understand if and how the service provider's contractual set up conforms to the standards the German company offers its EU customers.

The following guidance may help tackle these issues:

- Do not sign any commercial contract before you have ensured that the vendor is aware of EU data privacy requirements and is willing to adjust its data processing agreements to fit these requirements and your needs.
- Ask the U.S. vendor for internationally accepted certificates on data security and, if possible, for compliance with international/ German cloud standards such as ISO 27018 or BSI C5.
- Understand whether the entire chain of sub processors is able/willing to comply with the data processing agreements you need for the EU data privacy compliance.



A CLOSER LOOK:

THE SWEEPING BUSINESS IMPLICATIONS OF THE NEW CALIFORNIA DATA PRIVACY LAW

End of June 2018, California announced a new California Consumer Privacy Act ("CCPA"), an act that borrows heavily from a broad range of existing, global privacy and consumer protection rules and regulations. It is a privacy melting pot, expanding on existing California rules, including the Online Privacy Protection Act (CalOPPA), Shine the Light, and the so-called Internet Eraser law, and flavored heavily with EU General Data Protection Regulation (GDPR) style data-ownership and control rights. Thus, the CCPA is sometimes referred to as "California's GDPR," although there are significant differences between GDPR and the CCPA and companies doing business in California should not assume that they are CCPA-compliant just because they are GDPR-compliant or vice versa.

The current version of the CCPA was passed with great haste to avoid a deadline for certifying a more aggressive ballot initiative and we anticipate it will undergo further revision before it goes into effect in January 2020. However, even if some of the most complex features are ultimately revised, it's quite likely that the statute will substantially impact most mid- to large-size businesses and potentially cause seismic shifts in certain industries, such as adtech and data brokerage services. Companies are well advised to assess readiness, identify gaps, prioritize and remediate well in advance of the effective date.

The act applies to most companies with California-based assets or customers. As a threshold matter, the act applies to any "business" that (i) does business in California, (ii) collects California consumers' "personal information" (which includes persistent identifiers), and (iii) satisfies one or more of the following thresholds: (A) annual gross revenues over $25 million; (B) buys, receives, sells or shares (for commercial purposes) the personal information of 50,000 or more Californian consumers, households or devices; or (C) derives 50 percent or more of its revenues from selling consumers' personal information.

The CCPA significantly expands the definition of "personal information" to cover almost any consumer-related data that a company collects or maintains (including behavioral, profiling and tracking data with quite some ambiguities whether or not de-identified and aggregated data falls within the act's scope).

There are several pretty onerous provisions in the act. Most notably, the CCPA:

- requires consent from children age 13-16 to sell personal information.
- establishes first-in-kind data ownership and control rights, providing consumers with substantial rights to data transparency, access, portability, deletion and choice over data use and sales to third parties; and
- requires the development of consumer-facing compliance mechanisms and related protocols.

The CCPA does not have the potential for huge penalties like the GDPR, but it does provide for a limited private right of action for a data breach (that could be very attractive to the California plaintiff's bar) and public authorities can assess an enforcement penalty of USD 7,500 per violation.

Historically, we have seen other U.S. states follow California's lead by passing their own versions of similar privacy laws, which might potentially further complicate the U.S. privacy landscape.

3. TRADE SECRETS – WHY IT MATTERS SO MUCH IN THE UNITED STATES

Known as trade secrets, such pieces of proprietary and confidential information helps a company distinguish itself from its competitors, gain notoriety, and develop products and services that stand out from the pack while keeping a competitive edge. Understanding and navigating the trade secret regulatory landscape is of utmost importance for any German technology company coming to the U.S. where heightened competition, shorter product cycles and increased employee mobility have over the last couple of years added up to more trade secrets claims – and higher-stakes legal battles.

WHAT IS A TRADE SECRET?

A trade secret is confidential information of a commercial nature from which the holder derives an economic benefit. A trade secret may be a secret device, formula or process or customer lists or other business, financial or technological confidential information. Unlike patents, which require the disclosure of certain information, demand registration and respective fees from time to time, and will "only" offer protection for a certain period of time, owners benefit from trade secrets both in convenience as well as in a financial way: trade secrets are not limited in time, but, are protected ipso jure for as long as they remain confidential and do not need to be registered upon fees.

Nevertheless, it is often inevitable and necessary to disclose information to certain employees and to licensees during the course of business. Although absolute confidentiality is not practicable, owners of trade secrets must undertake all reasonable precautions against misappropriation risks by these persons to benefit from protection under trade secrets law. Although threats arise mostly from those who are granted access to trade secrets (in particular employees and licensees), third parties who illegally access trade secrets (or parts of it in an effort to engage in "reverse engineering") also pose a risk.

HOW ARE TRADE SECRETS PROTECTED AND ENFORCED?

In the United States, trade secrets are protected by state law, with many states observing the guidance of the United States Uniform Trade Secrets Act ("UTSA"). Violations of these rules will entitle the owner to bring forward civil lawsuits before state courts against the "thief." In addition, certain "thefts" of trade secrets may be punishable under criminal law, in particular the U.S. Economic Espionage Act.

The newly enacted United States Defendant Trade Secrets Act of May 2016 ("DTSA") further opened the doors of federal courts to trade secrets litigants and augmented existing protections. The U.S. Senate cited the mounting cybersecurity risks as the driving force behind the DTSA, as protection became increasingly difficult given the ever-evolving technological advancements. As state law resulted in state-to-state variation on a number of important issues, the DTSA is a step in the direction of homogeneity. Now a trade secret owner may file a petition in a Federal District Court alleging claims under both the DTSA and, if applicable, the UTSA as codified under state law. To satisfy the scope of DTSA's "interstate commerce" jurisdiction requirement is simple: any trade secret information related to a product or service that is sold or offered via internet is likely to fulfill the premise. The remedies set forth in the DTSA are largely adopted from the UTSA. The civil seizure remedy is, however, new. Under extraordinary circumstances, the plaintiff may obtain an order on an ex parte basis directing a federal marshal to seize from the defendant the allegedly misappropriated trade secret. This might be the case when the applicant will suffer "immediate and irreparable injury" in a way that other forms of extraordinary relief, such as temporary restraining orders, would not adequately address. This remedy has long been available to trademark infringement litigants under the Lanham Act, which may now provide for guidance in jurisprudence.

This broadened arsenal of far-reaching remedies makes managing trade secret litigation risks an ever more important topic for every technology company active in the United States, and we recommend obtaining legal advice early on to establish adequate compliance systems. The DTSA is also relevant for technology companies for another reason, as it provides guidance for employer-employee cases.

The DTSA now clearly answers the question of employee mobility, which has been subject to contested litigation under the UTSA. Contrary to the "inevitable disclosure doctrine," the court may not order an injunction that prevents a former employee from entering into a new employee relationship based on a showing that the former employee's knowledge of the employer's proprietary information is so comprehensive that the employer's trade secrets would inevitably be disclosed and used in the course of the former employee's new employment. Also, the DTSA must not conflict with existing state law that prohibits restraints on lawful profession, trade or business.

In addition, whistleblower immunity provisions provide for criminal and civil liability to any person who discloses a trade secret to a federal, state or local government official solely for the purpose of reporting or investigating a (mere) suspected violation of law (especially criminal statute, environmental regulation or labor standard). In case the employer retaliates against the employee, the DTSA permits the employee to disclose the employer's trade secret to her attorney and use it in any subsequent retaliation suit.

In addition, employers must comply with the notice requirement regarding this immunity in employment agreements entered into after the DTSA's enactment in May 2016.

STAY ON THE CUTTING EDGE WITH THE "*TRADE SECRETS WATCH*"

Orrick's blog "Trade Secrets Watch" offers the latest trade secret news and analysis from the U.S. and across the globe. It covers recent cases and proposed legislation, verdicts and settlements, practice tips, upcoming events, and other interesting trade secret tidbits. *Trade Secrets Watch* has established itself as one of the leading trade secret blogs since it launched in May 2013, with reprints and discussion of our blog posts in media such as *Bloomberg*, *Corporate Counsel*, *Law360*, and *The IP Litigator*.

Learn more at http://blogs.orrick.com/trade-secrets-watch/.

WHAT MUST OWNERS OF TRADE SECRETS DO?

Owners of trade secrets must take affirmative actions and use reasonable efforts to protect their confidential information and benefit from the aforementioned trade secrets laws. Once trade secret information is disclosed – whether intentionally or inadvertently – it ceases to be protected under trade secret law.

But what does that mean in practice? What is "reasonable?" The laws don't tell us. Like the "reasonable person" standard in negligence, courts are supposed to decide each case in the context of its unique facts. That said, looking back at several decades of decisions, we can get a good sense of the principles at work and also how they may be shifting as the business environment becomes more digital and more global. The good news is that the standard is flexible, taking into account the value of the information, the risk of loss or contamination, and the cost (in money and effort) of measures to reduce those risks. For most businesses, this means simply taking a close look at what drives your competitive advantage and then applying ordinary risk management analysis to define the broad outlines of a protection plan. In practical terms, this can lead to a variety of specific actions, including the basic ones you find on a lot of checklists with items like confidentiality agreements, IT system access controls, staff rules and training, and facilities security.

Otherwise employers are precluded from seeking recovery of attorneys' fees or other exemplary damages, which are granted by the DTSA to owners of trade secrets under certain circumstances. As a result, it is of utmost importance for employers to comply with the notice requirement.

So if you're following one of those checklists, you should be fine, right? Not necessarily.

Although judges historically have been forgiving of less-than-robust security measures, they now seem to be paying much closer attention to this issue and have even thrown out claims without trial where the trade secret owner has been sloppy in its practices. Naturally, as the risks increase, the market responds with tools and systems to prevent cyberattacks, or at least discover them early and frame an appropriate response. And government agencies, most notably the National Institute of Standards and Technology, have suggested frameworks for managing cybersecurity risks. It's not hard to imagine that these voluntary processes may, over time, be interpreted by courts as best practices, and even as minimum standards of conduct.

Overall, any owner of a trade secret should obtain proper advice on how to protect it early on. Owners will have to implement organization and technical security measures to limit access to internal information as well as apply appropriate trade secret and information security policies, potentially even with perpetual obligations toward employees. Finally, the notice of immunity under the DTSA is a "must have" in employment agreements.

TRADE SECRET THEFT IN THE CLOUD[4]

As cloud services have transformed modern business, they have also changed the way companies protect and enforce their trade secrets. Companies and their employees increasingly store data on cloud-based platforms. While these platforms can provide flexible and cost-effective storage options, they also present unique problems for tracking access to and use of company trade secrets. As a result, companies that allow employees to access company data remotely or from personal devices via cloud platforms should carefully consider the implications and weigh options for protecting company data that makes its way to devices and locations outside the company's direct control. Although courts and companies have at times struggled to keep pace with the rapidly evolving challenges surrounding the use of cloud-based software, some best practices have emerged from the body of case law addressing claims of cloud-based appropriation of trade secrets.

The Cloud's Risks to Trade Secret Owners: First, the risks: Innumerable companies worldwide use cloud applications like Dropbox, iCloud, Google Drive and Box to enable employees to work more flexibly and efficiently. Often, employers allow access to company cloud applications from employees' personal devices. But when an employee downloads information from the cloud to a personal device that is outside the company's control, the company may lose track of what subsequently happens to that information. In other instances, companies (especially start-ups) adopt a "bring your own cloud," or BYOC, policy permitting employees to use personal cloud accounts for company business. Under this approach, there is a risk that the employee may ultimately refuse the company access to a personal cloud account, even if it contains company information. The ease with which data may be transferred in a cloud-centric world compounds the difficulties of maintaining a handle on company data. Because no physical files are at issue in cloud-based transfers, massive amounts of data can be taken without any overtly suspicious behavior (*e.g.*, no employee is seen carrying boxes of files out of the office). This has led to an increase in cases alleging cloud-based theft.

While methods of protecting company information in the cloud are almost as numerous as the cloud services themselves, they typically fall into a handful of categories.

Site-Blocking Software: In response to the risks cloud storage poses to trade secrets, some companies utilize third-party software to block access to specific sites, including to cloud services. Among the problems with this approach is that there are too many cloud service applications out there to block. Moreover, there are other concerns with such an approach, including that it limits employees' abilities to use a diverse range of services for legitimate purposes. Thus, playing "whack-a-mole" by blocking various cloud services is unlikely to be successful on its own, as is any other purely technical solution.

4 The following chapter is based on an article that Amy Van Zant, Evan Brewer and Margaret Wheeler Frothingham from Orrick published in June 2018 in Law360.

Employee Agreements and Company Policies: Employee agreements, company trade secret and confidentiality policies deserve close attention when crafting a trade secret protection program intended to mitigate the risks created by cloud technologies (for more details on Confidentiality and Invention Assignment Agreements please see Chapter B.4 below). Such agreements and policies can serve as a first layer of defense and a basis for investigation and remedial action in cases of suspected trade secret misappropriation. There is no "one size fits all" best practices for such agreements and policies. But case law has shown that inserting trade secret protection clauses in employee agreements can be a key to enforcing trade secret rights even in circumstances where an employee might argue that she acquired the trade secrets through proper means, such as during the course of work. For example, in Prominence Advisors Inc. v. Dalton[5], the court dismissed Prominence's claim of trade secret misappropriation, finding that the employee had acquired information from the company's cloud-based systems during the course of his official duties. However, because the company's employee agreement required the return of all company policy upon leaving the company, Prominence was still able to pursue a breach of contract claim. The lesson here is clear: Even if a trade secret misappropriation or similar statutory or common law claim fails to protect a company's trade secrets, a well-crafted employee or confidentiality agreement may be a backstop to theft. Such provisions are low-cost means of ensuring an additional layer of protection beyond what is provided by default under the law, and an important tool in trade secret protection. Drafting employee agreements to protect trade secret information is all the more important because it remains unsettled what improper "acquisition" entails under the Computer Fraud and Abuse Act ("CFAA"). The Second, Fourth and Ninth Circuits have held that the CFAA prohibits only unauthorized access to information. In these circuits, a defendant can use information however she chooses without CFAA liability as long as her access was authorized. By contrast, the First, Fifth and Eleventh Circuits have held that the CFAA may also cover the unauthorized use of information, even if the defendant was authorized to access it. Depending on the circuit in which a company resides, its claims could meet different outcomes under the CFAA.

Five Best Practices for Avoiding Cloud-Based Theft: Employers should employ an array of solutions to combat theft through cloud technology, taking a comprehensive approach that considers the particular character of the business and its employees. Some companies may be in a place to implement a more lenient, "trust but verify" type approach that provides more flexibility. Others, such as those with highly sensitive trade secrets (for example, the proverbial "recipe for Coca-Cola") may need to take a more restrictive approach that locks down access and limits flexibility for the sake of absolute security. In striking the appropriate balance, companies should consider the following tools and procedures:

- Implement technical solutions when feasible. Blocking access to particular domains or services, or restricting access to certain files and repositories may be appropriate depending on the individual circumstances of the business.

- Employ surveillance and monitoring tools to the extent appropriate for the business. Search out and monitor unusual download or computer behavior, especially when an employee has given notice of intent to work for a competitor or has been terminated.

5 Prominence Advisors Inc. v. Dalton, No. 17 C 4369, 2017 WL 6988661 at *4 (N.D. Ill. Dec. 18, 2017).

- Verify compliance with company confidential information and computer use policies (see below). After an employee departs, companies should assess the risks of potential theft and consider investigating the employee's recent computer activity for illicit use of a personal cloud. While it is not practical to investigate every departing employee, suspicion of wrongdoing should trigger some level of investigation. Often, trade secret theft that goes undiscovered until too late could have been found by a prompt review of a departing employee's devices. In addition, upon employee departure or termination of employment agreement, company-owned employee cloud accounts should be promptly disabled and companies should verify that company data stored on employees' personal cloud accounts has been destroyed.

- Implement and require employees to sign acknowledgement of a comprehensive written company policy that defines the scope of the company's and the employees' rights and obligations regarding trade secrets. This should contain both standard provisions regarding the company's trade secrets and specific provisions governing the use of cloud storage, company-issued devices and personal devices. Not only will such policies place employees on notice of their responsibilities, but they will place the company on firm footing when and if it ever must investigate or litigate trade secret theft.

- Include trade secret provisions in employee agreements. Companies should consider incorporating the following into the company's standard employment agreement, its written company policies or both:

  — Require employees to maintain company trade secret information as confidential, and prohibit disclosure of company trade secrets to third parties.

  — Identify what company data can and cannot be transferred to the cloud.

  — State whether employees are permitted to use personal devices to access company cloud services and whether the use of personal cloud storage services to store company information is prohibited.

  — Define the company's right to access, retain, destroy and/or delete data or information from an employee's personal devices and cloud accounts.

  — Require employees to identify and provide login information for any personal cloud solutions used for work purposes.

  — Specify a process for preserving and producing data from personal clouds.

  — Require the return of all company information at the end of employment.

4. 13 KEY EMPLOYMENT CONSIDERATIONS

Although many German entrepreneurs have heard about U.S. labor law-related disputes that can become mission-critical for young technology companies and have at least a vague idea that U.S. labor law practices are very different from what they are familiar with in Germany, there are many pitfalls that await the unwary. Employers can fall into a myriad of costly employment-related traps. Numerous state and federal laws impact the hiring process and apply a wide variety of employment-related protections, including to discipline and termination issues.

For many start-up and emerging companies developing technology, the issues associated with the creation of intellectual property by employees and consultants are crucial. Employment litigation is expensive, disruptive and distracting. Therefore, emerging companies and start-ups should implement appropriate steps and agreements from the outset. In this chapter we discuss 13 key employment and labor law issues for start-up and emerging companies in the U.S. and give practical guidance how to navigate legal challenges and pitfalls[6].

6 The following paragraphs are taken from an article from our partners Lynne C. Hermle and Michael D. Weil (together with their co-author Richard D. Harroch) that was published in *Forbes* under the title **"13 Key Employment Issues For Startup and Emerging Companies"** on January 10, 2018 (www.forbes.com/sites/allbusiness/2018/01/10/13-key-employment-issues-for-startup-and-emerging-companies/#5a7e170f68b4).

KNOW WHAT HIRING QUESTIONS YOU MAY NOT ASK

Federal and state laws prohibit employers from making hiring decisions based on protected categories: gender, race, age, color, religion, disability and others. Asking the wrong questions could lead to a discrimination claim against the company, even if decisions are not made on that basis. Here are examples of the types of questions to stay away from:

- How old are you?
- What is your religion?
- Do you have any medical conditions we should be aware of?
- Have you ever been arrested?
- Do you have any disabilities that would hinder you in performing the job?
- Have you had any recent illnesses or operations?
- Are you married?
- Do you have children or plan to have children?
- How long do you plan to work until you retire?
- Do you drink or smoke?
- What is your political affiliation?
- Is English your first language?
- What type of discharge did you receive from the military?
- What country are you from?
- Where do you live?
- Do you take drugs?

Some of these may be obvious. But these questions may also be prohibited:

- What is your maiden name?
- Do you own or rent your home?
- Where is your family from?
- What was the date/type of termination of your last employment?
- Can you give me the name of a relative to be notified in case of emergency? (The problem is asking for the name of a relative. But you can ask "In case of an emergency, whom can we notify?")

ASK EACH CANDIDATE TO FILL OUT AN EMPLOYMENT APPLICATION

An employment application can serve several useful purposes. First, it provides key information that will enable the employer to determine whether an initial or further interview makes sense. Second, it serves as a representation and warranty from the candidate as to the truthfulness of the information provided (which may be useful later on if problems arise).

And, the information provided can facilitate reference checking. There are plenty of examples on the web of employment applications, including a comprehensive one at AllBusiness.com. In any case, be sure you don't have any of the prohibited inquiries (including arrest questions) on the application.

PERFORM A COMPREHENSIVE REFERENCE CHECK BEFORE YOU HIRE THE EMPLOYEE

Many employers conduct a limited and incomplete reference check as part of the hiring process, often leading to issues with the candidate's inability to perform their required duties or to get along with others.
A comprehensive reference check includes:

- Verification of job titles and dates of employment.
- Verification of educational degrees and dates of attendance at schools.
- Verification of starting and ending salary.
- Verification of job role and responsibilities.
- Inquiry as to why the applicant left the prior employer.
- Conversations with prior supervisors as to the applicant's strengths and weaknesses.
- Inquiry as to the applicant's ability to get along well with other employees and customers.
- Inquiry as to the applicant's ability to take on the new role.
- Inquiry as to punctuality or absenteeism issues.
- Reference checks with other people not listed by the applicant as a reference.

The purpose of these checks is to make sure that the applicant will fit into the company's culture and to ensure that the applicant has been truthful in their resume and employment application. However, the process is carefully regulated by the federal government (through the Fair Credit Reporting Act) and the laws of many states; failure to follow the highly technical process can lead to class action lawsuits. Consider consulting legal counsel.

USE A GOOD FORM OF OFFER LETTER OR EMPLOYMENT AGREEMENT

Oral agreements often lead to misunderstandings. If you plan to hire a prospective employee, use a carefully drafted offer letter, which the employee is encouraged to review carefully before signing.

For senior executives, a more detailed employment agreement often makes sense. A good offer letter or employment agreement will address the following key items:

- The job title and role of the employee.
- Whether the job is full time or part time.
- When the job will commence.
- The salary, benefits, and any potential bonuses.
- Whether the position is "at will" employment, meaning either party is free to terminate the relationship at any time without penalty (although employers may not terminate employees for legally prohibited reasons, such as for age discrimination or retaliation from sexual harassment allegations, etc.).
- Confirmation that the "at will" agreement may not be changed unless signed by an authorized officer of the company.
- Confirmation that the employee will need to sign a separate Confidentiality and Inventions Assignment Agreement (described below).
- If the company chooses, a statement that any disputes between the parties will be resolved solely and exclusively by confidential binding arbitration (also discussed below).
- Any stock options to be granted to the employee and the terms of any vesting (details usually laid out in a separate stock option agreement).
- To whom the employee will report.
- Language stating that the offer letter constitutes the entire agreement and understanding of the parties with respect to the employment relationship, and that there are no other agreements or benefits expected (unless additional provisions are laid out in a handbook, which should be referenced if so).

Companies should ensure that the employee and the Company sign the letter, the Confidentiality and Invention Assignment Agreement, any stock option agreement, and any first day paperwork (such as the IRS W-4 Form for withholding and the I-9 form mandated by law).

The following is an example of a form of employee offer letter:

[Name of Company]

[Date]

Re: Terms of Employment

Dear _____:

We are pleased to inform you that [Name of Company] (the "Company") has decided to make you this offer of employment. This letter sets forth the terms of the offer which, if you accept, will govern your employment.

1. Position; Duties. Your position will be _____, reporting to the _____ of the Company. Your duties and responsibilities will be as designated by the Company, with an initial focus on (i)_____

2. and (ii)_____.

2. Full-Time Employment. The employment term will begin on _____, 20__.

3. Compensation. Your compensation will be USD___a year, paid [every two weeks] consistent with the Company's payroll practices. Your package will include participation in the health and other benefit plans of the Company pursuant to their terms as may be amended by the Company from time to time. You will be entitled to ____weeks paid vacation (equivalent of business days) for each year of full employment. Unused vacation time should be taken and may not be carried over into subsequent years.

4. Stock Options. Subject to approval of our Board of Directors, we expect you will be granted options to acquire___ shares of the Company's Common Stock, vesting over a [four (4)] year term with one (1) year cliff vesting f¼1/4th of the options. The options are expected to be granted at a strike price of USD__ per share. The terms and conditions of your stock options are contained in a Stock Option Agreement of today's date and must be executed by you and returned to us immediately.

5. Employment at Will. Our employment relationship is terminable at will, which means that either you or the Company may terminate your employment at any time, and for any reason or for no reason. Our at will agreement can only be modified by a writing signed by both you and the CEO of the Company.

6. Confidentiality and Invention Assignment Agreement. You will be subject to the Company's Confidentiality and Invention Assignment Agreement, which is enclosed with this letter and must be signed and returned by you before any employment relationship will be effective.

7. Certain Acts.During employment with the Company, you will not do anything to compete with the Company's present or contemplated business. You will not engage in any conduct or enter into any agreement that conflicts with your duties or obligations to the Company. You will not during your employment or within one (1) year after it ends, directly or indirectly solicit any employee, agent, or independent contractor to terminate his or her relationship with the Company.

8. Representations. You represent that you are aware of no obligations legal or otherwise, inconsistent with the terms of this Agreement or with your undertaking employment with the Company. You will not disclose to the Company, or use, or induce the Company to use, any proprietary information or trade secrets of others. You represent that you have returned all proprietary and confidential information belonging to all prior employers. You also represent and warrant that all information provided to the Company (including any information in your resume and any Employment Application) is true, correct, and complete.

9. Arbitration.

a) Disputes can arise even in the best of relationships. Rather than fighting it out in court, both you and the Company agree that any controversy, claim, or dispute arising out of or relating to this Agreement or the employment relationship or your compensation, either during the existence of the employment relationship or afterwards, between the parties hereto, shall be settled solely and exclusively by confidential binding arbitration in the city in which you work.

b) Such arbitration shall be conducted in accordance with the JAMS Employment Rules & Procedures (which can be reviewed at http:www.jamsadr.com/rules-employment-arbitration) in existence at the time of the commencement of the arbitration, with the following exceptions if in conflict: The Company will pay the arbitration filing fees and the arbitrator's fees; one arbitrator shall be appointed by JAMS; and arbitration may proceed in the absence of any party if written notice (pursuant to the JAMS' rules and regulations) of the proceedings has been given to such party.

c) The parties agree to abide by all decisions and awards rendered in such proceedings.

d) You and the Company agree that any claim for breach of this Agreement and any claim regarding or related to your employment, including disputes regarding compensation, discrimination, wrongful termination, harassment, and any and all other conflicts or claims will be resolved solely and exclusively by confidential final and binding arbitration on an individual basis only, and not on a class, collective, or private attorney general representative basis on behalf of other employees, to the extent not prohibited by applicable law.

e) We both agree to waive any rights to a jury trial or a bench trial in connection with the resolution of any dispute under this Agreement (although both of us may seek interim emergency relief from a court to prevent irreparable harm pending the conclusion of any arbitration).

f) This Section 9 arbitration provisions shall not apply to the following matters: (1) claims for workers' compensation; (2) claims for unemployment compensation benefits; (3) claims or charges before an administrative agency having jurisdiction over the matter; or (4) claims that are forbidden to be arbitrated as a matter of law.

g) Any dispute or claim concerning the scope or enforceability of the arbitrations provisions of this Section 9 shall be determined exclusively by an arbitrator pursuant to the procedures set forth above.

h) The arbitrator shall have the power to award all relief available in law or equity requested by the parties and supported by credible, relevant, and admissible evidence.

i) Arbitration is not a mandatory condition of your employment. If you wish to opt out of the arbitration provisions of this Section 9, you must notify the Company by email to _____@____.com, stating your decision to opt out, within 10 days of your signing this Agreement.

10. Miscellaneous. Upon your acceptance, this letter will contain the entire agreement and understanding between you and the Company and supersedes any prior or contemporaneous agreements, understandings, term sheets, communications, offers, representations, warranties, or commitments by or on behalf of the Company (oral or written). The terms of your employment may in the future be amended, but only by writing and which is signed by both you and, on behalf of the Company, by a duly authorized executive officer, provided, however, that you agree to comply with the provisions of the Company's Employee Handbook, as may be amended or adapted by the Company from time to time. In making this offer, we are relying on the information you have provided us about your background and experience, including any information provided us in any Employment Application that you may have submitted to us. The language in this letter will be construed as to its fair meaning and not strictly for or against either of us. If any provision of this Agreement is held invalid, in whole or in part, such invalidity will not affect the remainder of such provision or the remaining provisions of this Agreement. This Agreement is governed by [State] law (without regard to conflicts of law principles) and the Federal Arbitration Act (FAA), but in case of a conflict the FAA controls.

If these terms are acceptable, please sign in the space provided below and return this letter to us. Again, we're very excited to have you join the Company.

Yours truly,

[Name and Title]

IMPORTANT

I agree that I have been given a reasonable opportunity to read this Agreement carefully. I have not been promised anything that is not described in this Agreement. The Company encourages me to discuss the Agreement with my legal advisor. I have read this Agreement, understand it, and I am signing it voluntarily. By signing the Agreements, I understand that the parties are agreeing to arbitration for any disputes as set forth above.

Agreed and Accepted:

[Name]

ADOPT A WELL-DRAFTED ANTI-HARASSMENT AND ANTI-DISCRIMINATION POLICY

The company should have a carefully drafted anti-harassment and anti-discrimination policy (which is required by some state laws and expected by many jurors if litigation were to arise).

Helpful policies typically run 2-3 pages in length and samples can be obtained from experienced employment lawyers or HR consultants. A good policy typically addresses the following:

- The company's zero tolerance of any forms of harassment, discrimination, bullying, or violence in the workplace.
- The definition of sexual and other types of harassment or discrimination (*i.e.*, based on race, color, religion, national origin, age, disability, etc.).
- Examples of conduct constituting prohibited harassment.
- Rights of the employees to complain about harassment, discrimination, and retaliation, and to whom such complaints should be made (consider making HR the designated recipient of complaints to ensure they are properly handled).
- The company's policy to investigate claims.
- Assurance that the employer will protect the confidentiality of complaints to the extent possible.
- Strong prohibitions on any retaliatory conduct.
- The disciplinary actions that may be taken upon determination that the policy has been violated.
- State and federal remedies available to the employee.

The company should distribute the policy, ideally annually, to all employees with a cover email or other communication insisting on its importance and the need for compliance.

A CLOSER LOOK:

THE "METOO" DEBATE AND NINE KEY RECOMMENDATIONS FOR EMPLOYERS[7]

How a company reacts to a complaint of sexual harassment or discrimination significantly impacts the legal exposure, disruption, effect on the company's reputation, length of the dispute, and costs incurred. Below are key steps a company can take in responding to sexual harassment or discrimination claims, both with respect to addressing workplace allegations as well as dealing with any resulting litigation. While legal and policy considerations are key, effective communications are equally essential, and a team of HR, legal, and (where appropriate) communications professionals should coordinate carefully with senior management on the company's response.

7 The following paragraphs are taken from an article from our partner Lynne C. Hermle that was published in *Forbes* under the title **"15 Key Steps For Companies Responding To Sexual Harassment Or Discrimination Allegations"** on November 13, 2017 (www.forbes.com/sites/allbusiness/2017/11/13/15-key-steps-for-companies-responding-to-sexual-harassment-or-discrimination-allegations/#34adaa9b4582).

A CLOSER LOOK:

THE "METOO" DEBATE AND NINE KEY RECOMMENDATIONS FOR EMPLOYERS (CONT.)

LAWYER UP!

In the United States, sexual harassment or discrimination complaints can lead to serious liability, including punitive damages designed to punish the company for inappropriately handling the complaints. The company may face significant liability even if a low level supervisor fails to comply with company rules and policies. Not all of the proper responses to these claims are intuitive and many require knowledge of complex applicable laws and regulations. Thus, the company should involve outside legal counsel experienced in handling such claims as soon as possible to navigate the thicket of related legal issues. Counsel can provide guidance on compliance with legal requirements for the response as well as assist the company in determining whether early resolution is advisable or possible.

With the assistance of legal counsel, the company can also take the appropriate steps to ensure that communications with executives, board members, and employees are protected by attorney-client privilege. To protect that privilege, communications with the company's legal counsel should be restricted to those individuals with a legitimate need to know and include a subject line that reads "Confidential and Subject to Attorney-Client and Work Product Privileges."

TAKE APPROPRIATE ACTION DURING AND AFTER THE INVESTIGATION

A full investigation into sexual harassment or discrimination often takes time, and it may be appropriate for the employer to take immediate steps with respect to the employee who raised the concerns. Protective measures may include, depending on the circumstances, the following;

- Placing the alleged wrongdoer on paid or unpaid leave, pending the outcome of the investigation;
- Allowing the complainant paid time off during the investigation;
- Altering work assignments so that an alleged harasser does not work directly with or supervise the complainant; and
- Ensuring that all supervisors understand that retaliation will not be allowed.

If the company determines that a policy was violated and inappropriate conduct occurred, it should take appropriate disciplinary action. The correct discipline, depending on the severity of the situation, can include warning, counseling, impact on bonus, impact on future compensation increases, suspension, or immediate firing of the wrongdoer. It is important to document the discipline carefully, although specifics about the investigation should not go into personnel files.

COOPERATE WITH GOVERNMENT AGENCIES

The Equal Employment Opportunity Commission ("EEOC") strongly advises employers to promptly investigate complaints of harassment or other unfair employment practices. But the EEOC or similar state agencies may conduct their own investigation related to employee claims, typically after the employee files an administrative "charge" accusing the employer of discrimination.

If the EEOC or other government agencies do become involved in reviewing a complaint, the company must cooperate. The governmental agency likely will require a response to the complaint and production of relevant documents (typically those related to the personnel actions at issue). The cooperation and document production should be coordinated with legal counsel, as the company's response may lead to action by the agency or cause problems in future litigation.

CONSIDER WHETHER THE COMPLAINT CAN BE RESOLVED THROUGH ARBITRATION

If litigation is threatened or filed in court, the company should determine whether any arbitration agreements might apply to the claim. Arbitration provisions may be present in hiring letters, employment agreements, benefit plans, bonus agreements, employee handbooks, and documents created by outside HR providers.

A CLOSER LOOK:

THE "METOO" DEBATE AND NINE KEY RECOMMENDATIONS FOR EMPLOYERS (CONT.)

DON'T RETALIATE

The company should ensure that it does not retaliate against a complaining employee (or a witness involved in the investigation), even if the initial complaint proves to be unfounded. Retaliation claims are often more difficult to defend against than harassment or discrimination allegations, in part because jurors tend to believe that those who are falsely accused have a natural motive to strike back. Retaliation can include many negative acts, including:

- Termination of employment
- Demotion
- Change in responsibilities
- Disciplinary action
- Transfer of the employee to a less desirable location
- Compensation or benefits reduction
- Change of shift hours or work area
- Isolating the employee by leaving them out of company activities
- Giving a performance evaluation that is more negative than it should be
- Making the employee's work more difficult (such as purposefully changing work schedule to conflict with the employee's family responsibilities)
- Threats to do any of the foregoing

BE CAREFUL WITH TEXTS AND EMAIL

After an employee lodges a harassment or discrimination allegation, executives often exchange a flurry of emails or texts responding to and attempting to address the problem. This can be extremely problematic in future litigation, as the shock or concern may lead to emotional and negative reactions to the claim. A company may be required to turn over these emails and texts (and any other forms of communications, such as Slack messages and voicemails) in the course of the litigation. These communications can come back to haunt the company, as the plaintiff's counsel will attempt to use these as evidence of the company's bad faith, complicity, or retaliatory motive.

PRESERVE DOCUMENTS

Once a claim is made, it's important for the company to put a "legal hold" in place. This means that any relevant emails, memos, and other documents must be preserved and not deleted or destroyed, in anticipation of potential litigation. Failure to protect these documents (even inadvertent and unintentional destruction through automatic email deletion processes) can lead to punishment from the court. This can include both monetary fines and evidentiary sanctions, which can adversely affect a company's ability to fully defend itself against the claims.

DEVELOP A MEDIA STRATEGY

With the development of online court dockets, reporters now have access to many litigation filings. A newly filed lawsuit will soon appear on an online court site visible to the press, and the media (which scours the filings for lawsuits of interest) may begin to report very quickly—possibly even before the company has been served with it. If the company does not have an experienced spokesperson, such as a communications or PR director, the company will need to get its media house in order. Because the plaintiff may seek to rely upon the company's statements to the press or employees to show bad faith or malice (or possibly defamation), these must be carefully drafted, reviewed, and re-reviewed.

A CLOSER LOOK:

THE "METOO" DEBATE AND NINE KEY RECOMMENDATIONS FOR EMPLOYERS (CONT.)

IF YOU SETTLE, INCLUDE THESE PROVISIONS IN A SETTLEMENT AGREEMENT

If the company decides to settle the sexual harassment or discrimination claim, it's important to have in place a well-drafted and legally enforceable Settlement Agreement. The key terms of such agreements typically include:

- The consideration payable to the complaining party (all cash up front? installments payable over time? reimbursement of COBRA costs? non-monetary terms, like recommendation letters?)
- Whether the complaining party continues employment or resigns, and, if so, when
- A complete release and waiver of all claims, known and unknown, against the company and its officers, employees, directors, shareholders, and agents (note that in California and certain other states, prescribed statutory language is necessary to validly waive unknown claims)
- Any obligation of the complaining party to keep the terms of the Settlement Agreement confidential
- An obligation of the complaining party from future disparagement about the employer and its officers, directors, shareholders, employees, and agents
- A covenant of the complaining party to never sue or bring any action related to the claims released
- The method for resolution of any disputes under the Settlement Agreement (the company will often elect for such disputes to be handled exclusively through confidential binding arbitration)
- An "integration clause" stating that the Settlement Agreement represents the entire understanding and agreement of the parties, and supersedes any prior or contemporaneous understanding or agreement of the parties with respect to the subject matter of the Settlement Agreement
- A disclaimer of any liability or admission by the company with respect to the underlying allegations
- If litigation has been filed, a provision for dismissal and withdrawal of claims "with prejudice" (so that a similar claim can never be filed again)
- A statement that the agreement does not waive claims that cannot be waived as a matter of law
- The employee's waiver of any right to future employment with the employer or its affiliates

PROMPTLY AND THOROUGHLY INVESTIGATE ANY SEXUAL HARASSMENT OR DISCRIMINATION COMPLAINTS

The company should promptly investigate sexual harassment or discrimination complaints (including those which may initially appear to be meritless). Failure to treat a complaint seriously can exacerbate the problem and the liability to the company. Given

Investigations should be conducted by persons with training and experience and who have the ability to be neutral and impartial (*i.e.*, who don't report to or have relationships with those individuals involved in the complaint). Legal counsel should provide advice as needed, including on any thorny evidentiary or credibility issues which could arise during the investigation.

The investigator should create an initial plan for thoroughly analyze the complaints, ideally in consultation with counsel. Here are some basic steps which may be appropriate for that plan, depending on the facts:

- Determination of the appropriate scope of the investigation.
- Interviews with the complaining party.
- Interviews with the accused employee.
- Interviews with other employees and third parties (contractors, outside witnesses, etc.) who may have relevant information.
- Review of emails, memos, and other relevant communications.
- Review of the personnel files of the parties (including any prior disciplinary write-ups).
- If needed, consideration of how to resolve credibility in assessing conflicting reports.
- Assessment of whether the initial scope of the investigation needs to be broadened.
- Action taken to address the concerns raised, potentially including training and discipline, which should be clearly documented.
- Determination of the form of any report that should follow.

Here are some tips for an appropriate investigation:

- Determine the appropriate scope of the investigation; the scope will vary depending upon the allegations and should be reassessed if facts change.
- Choose an investigator who has good people skills and judgment. Both will be important in almost every investigation. If you don't have a qualified neutral candidate inside, hire an experienced one from outside. One good resource is the Association of Workplace Investigators.
- If the initiation of the investigation is delayed (for example, because the appropriate internal investigator is traveling or the company is searching for an appropriate outside investigator), document the reasons for the delay. The company may need to explain in litigation, possibly years down the road, why it did not begin to investigate immediately.
- The investigator should coordinate activities with legal counsel from the outset so that the company can determine whether the investigation will be privileged. This is especially important for the drafting of memos or notes associated with the investigation.
- The investigator should review company policies or procedures in place for dealing with harassment or discrimination.

Employee handbooks often include such procedures (for example, they may identify who is responsible for investigating or pertinent timelines), and you don't want to make the situation worse by not following the company's own articulated policies.

- Assure the complaining party at the outset that the complaint will be treated seriously, that there will not be any retaliation for raising it, and that any concerns about retaliation should be brought to the investigator's attention immediately so that they can be addressed.

- Instruct the accused not to contact the complainant regarding the complaint, and not to engage in conduct that is – or even might be viewed as – retaliatory. And if the accused violates the instructions (which happens regularly), take action immediately. It is not unusual for an employee or executive to be terminated for violating these instructions in the course of an investigation.

The U.S. Equal Employment Opportunity Commission ("EEOC") provides examples of questions that may be helpful in questioning the complainant and other witnesses, as well as other information helpful for the investigation. See Enforcement Guidance on Vicarious Employer Liability for Unlawful Harassment by Supervisors.

The investigator needs to keep an open mind when gathering and reviewing information, and to refrain from coming to a conclusion until all relevant data has been reviewed and assessed.

Encourage all involved to maintain the confidentiality needed for a thoughtful investigation while avoiding heavy-handed mandates (which might lead to National Labor Relations Board complaints about the employee's abilities to share workplace concerns).

Consider asking the complainant at the conclusion of the interview what she hopes will happen as a result of the investigation (one option: "how would you like to see the situation resolved?"). The company is not required to comply with unreasonable demands, but some requests (for example, a transfer, additional training, time off) may be helpful in resolving the concerns constructively.

Fairness is important. The investigation must be evenhanded, and both be fair—and appear to be fair—to all involved. The Guiding Principles for Conducting Workplace Investigations prepared by the Association of Workplace Investigators contains additional helpful advice.

MAKE SURE ALL EMPLOYEES SIGN A CONFIDENTIALITY AND INVENTION ASSIGNMENT AGREEMENT

Companies pay employees to come up with ideas, work product, and inventions that are useful to the business. Employees have access to a great deal of their company's confidential information, which can be highly valuable, especially in technology companies.

One basic way to protect proprietary company information is through a Confidentiality and Invention Assignment Agreement. This agreement deals with the confidentiality issues, but it can also provide that the ideas, work product, and inventions that the employee creates which are related to company business belong to the company – not the employee.

A good Employee Confidentiality and Invention Assignment Agreement will cover the following key points:

- The employee may not use or disclose any of the company's confidential information for her own benefit or use, or for the benefit of others, without authorization.
- The employee must promptly disclose to the company any inventions, ideas, discoveries, and work product related to the company's business that she makes during the period of employment.
- The company is the owner of such inventions, ideas, discoveries, and work product, which the employee must assign to the company.
- The employee's employment with the company does not and will not breach any agreement or duty that the employee has with anyone else, nor may the employee disclose to the company or use on its behalf any confidential information belonging to others.
- Upon termination of employment, the employee must return any and all confidential information and company property.
- While employed, the employee will not compete with the company or perform any services for any competitor of the company.
- The employee's confidentiality and invention assignment obligations under the agreement will continue after termination of employment.
- The agreement does not by itself represent any guarantee of continued employment.

Venture capitalists and other investors in start-ups expect to see that all employees of the company have signed such agreements. In an M&A transaction where the company is sold, the buyer's due diligence team will also be looking for these agreements signed by all employees. Similarly, it will be appropriate that all consultants of the company also sign a Confidentiality and Invention Assignment Agreement.

MAKE ARBITRATION YOUR DISPUTE RESOLUTION OPTION

Arbitration is usually quicker and cheaper than litigation. An arbitrator tends to be more dispassionate and more reasoned in the analysis of employment claims than most juries, which are often composed of employees with their own prior employment disputes. Arbitration can usually be handled confidentially, whereas lawsuits are public resulting in potentially adverse publicity (especially these days, as the media scrutinizes court dockets for juicy stories). And it may move faster than a lawsuit. On the other hand, the employer may be required to pay for the arbitrator's fees. For more details on the higher litigation risk in the U.S., please see Chapter B.6 below.

To ensure that employment disputes are resolved in arbitration, the company should have a well-drafted arbitration clause in offer letters, employment agreements, the employee handbook, and any benefit plans (stock option, bonus and Restricted Stock Unit plans, for example) for which it wishes to arbitrate disputes.

A well-drafted arbitration clause provides:

- That any disputes between the company and the employee will be handled solely and exclusively by confidential binding arbitration.
- What arbitration rules will apply, usually the rules of the American Arbitration Association or JAMS, in existence at the time of the commencement of the arbitration, with a citation to the rules (for example: "*You and the company agree to bring any dispute in arbitration before JAMS, pursuant to the JAMS Employment Rules & Procedures in effect at the time of the commencement of the arbitration, which can be reviewed at www.jamsadr.com/rules-employment-arbitration*").
- Who will pay the arbitrator's fees (in some places, including California, the employer must pay the fees as a matter of law).
- Where the arbitration will be held (ideally where the employee works).
- Waiver of any jury trial or bench trial.

To be enforceable, the arbitration agreement must not contain terms the courts find "unconscionable," such as limitations on damages or fees the arbitrator may award. Some matters, such as workers' compensation or EEOC complaints, may not be subject to arbitration.

PROPERLY CLASSIFY WORKERS AS EMPLOYEES OR INDEPENDENT CONTRACTORS

Both emerging and established companies face the issue of properly classifying workers as employees or independent contractors. It's critical to get this right. Class action lawsuits are filed daily attacking the classification of workers as contractors, and the potential damages and penalties can be enormous.

Employees and contractors are paid differently. Generally, the company must withhold income taxes, withhold and pay social security and medicare taxes, observe wage and hour laws, and pay unemployment tax on the wages of employees. On the other hand, employers generally are not required to withhold or pay taxes on payments to independent contractors, pay overtime compensation, or comply with other payroll and related issues applicable to employees. The general idea behind the difference is that the contractor will often have her own business, work for other companies, have expertise that is not subject to detailed control and supervision of the company, and may want the flexibility of setting hours and working arrangements.

The savings to a company by properly designating a worker as an independent contractor could be 20-40% of the labor costs. However, that savings will be quickly eaten up by challenges and claims from the government (which wants the tax payments) and lawyers for the workers.

The IRS takes the position that in determining whether a person is an employee or independent contractor, the key factor is the degree of control the company exerts over the process. Here are some of the factors which might indicate the worker should be classified as an employee:

- The worker is required to work a designated schedule of hours.
- The worker is required to work at the employer's place of business.
- The worker only provides services to one company.
- The company controls or has the right to control how the worker performs the service.
- The company provides the worker tools, supplies, office space, or equipment needed to do the job.

These factors may that indicate the worker may properly be classified as an independent contractor:

- The worker sets her own hours.
- The worker has licenses, insurance, and other indicators of a separate business.
- The worker provides services to more than one company.
- The worker works relatively independently.
- The worker has the authority to decide how to go about accomplishing tasks.
- The worker incurs the costs of performing the services.
- The worker has the opportunity for profit or loss from the work performed.

BE AWARE OF WAGE AND HOUR ISSUES

Employers routinely make mistakes related to wage and hour issues. These mistakes can lead to significant liability. The Fair Labor Standards Act sets the majority of wage and hour law at the federal level; some states, especially California, have passed wage and hour statutes and regulations that are stricter or contain more requirements than federal law does. Common mistakes include:

- Not complying with minimum wage standards.
- Improperly classifying employees as exempt from overtime laws.
- Failing to pay overtime to non-exempt employees.
- Failing to properly calculate an employee's overtime rate.
- Paying employees only for their scheduled work hours if the employer is aware that employees often work before or after their scheduled hours.
- Allowing employees to accumulate "comp time" instead of paying them for overtime.
- Not allowing legally mandated breaks.
- Not paying employees in a timely manner, particularly departing employees.
- Failing to accurately report wages and hours on pay stubs and other required records.
- Improperly deducting wages from an employee's compensation.

IMPLEMENT AN APPROPRIATE POLICY REGARDING USE OF SOCIAL MEDIA BY EMPLOYEES

It's important to establish a policy on social media that balances the desire of the company to avoid potential liability and unwanted attention with the employees' First Amendment and other rights. Such a policy will often describe what must never be shared on social media, such as confidential customer information, non-public financial information of the company, and other sensitive information. Sample social media policies are available on the web, such as the HP Blogging Code of Conduct, the LA Times Social Media Guidelines, the Intel Social Media Guidelines, the Coca-Cola Online Social Media Principles, the Dell Global Media Social Policy, and the Nordstrom Social Media Employee Guidelines.

MAINTAIN PROPER DOCUMENTATION CONCERNING EMPLOYEES AND HR

Companies are often sloppy in maintaining the proper employee/HR-related documentation. This can become problematic if the company is pursuing financing, is involved in an M&A activity, or is involved in litigation with an employee or regulatory agency. Here is a compendium of the types of documentation the company should consider maintaining:

- Job applications and resumes
- Employee offer letters
- Employment agreements
- IRS W-4 forms (Employees' Withholding Allowance Certificate)
- Form I-9 completed by all employees (eligibility of the employee to work in the U.S.)
- Anti-harassment and discrimination policy
- Employee handbook
- Stock option plan and agreements with all option holders
- Benefit plans
- Employee personnel files (including performance appraisals)
- Employee complaints
- Worker's compensation documents
- Emergency contacts
- Records of any disciplinary proceedings taken against employees
- Social media policy for employees
- Code of conduct policy for employees
- Compensation and bonus history
- Employee-related posters mandated by law to be posted in the workplace
- Employee termination notices
- PTO tracking records

Some software solutions, such as ComplyRight, Namely, Zoho, and others can be used to streamline hiring, onboarding, and employee records management through an online dashboard.

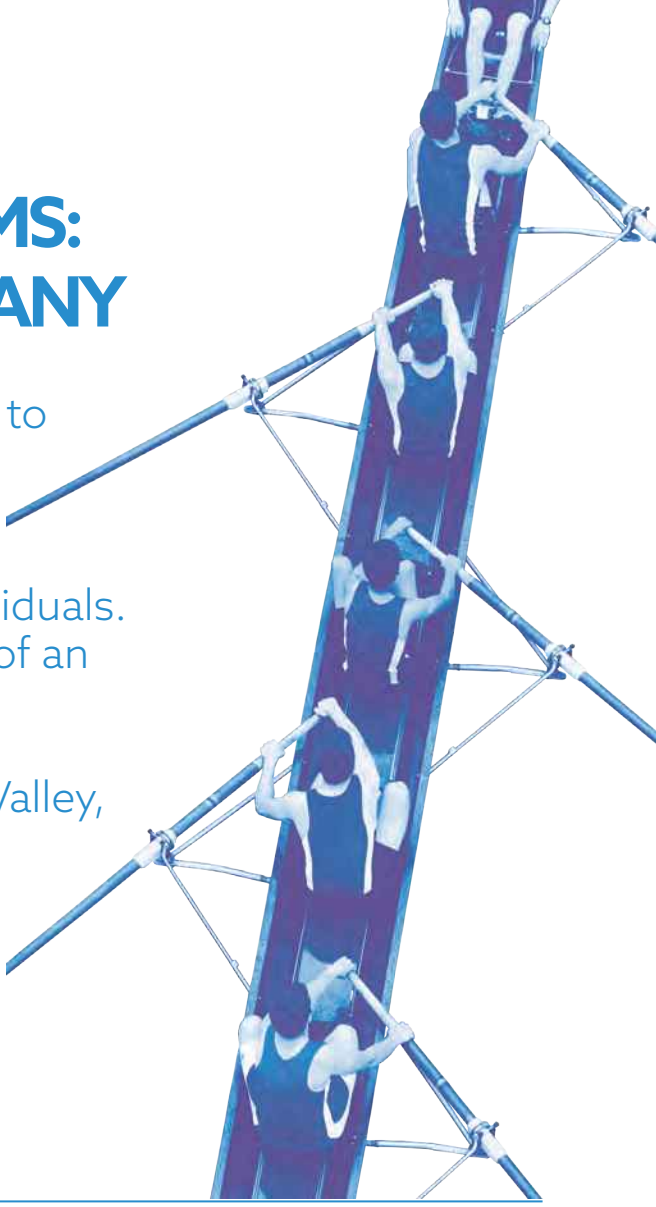
TAKE THESE STEPS BEFORE FIRING AN EMPLOYEE

Terminating an employee, even an "at will" employee, entails legal risk if not properly handled and documented. Various laws may prohibit termination based on gender, race, age, disability, religious preference, absenteeism due to jury duty or military service, violations of public policy, retaliation for sexual harassment or discrimination allegations by the employee, and other circumstances.

Here is some practical advice on what to do in connection with terminating an employee:

- Make sure you have an employee handbook or set of policies in place, with disciplinary policies. Clear violations of appropriate company policies can support an employee termination.
- If the employee has a history of poor performance or violation of company policy, make sure she has been notified and that this is included in the employee's personnel file. A warning may be more appropriate than an outright firing for the first problem with the employee.
- Investigate the situation as necessary to justify the termination.
- Review any employee offer letter or employment agreement to ensure there aren't steps or notices you have to undertake.
- Consult with employment counsel before termination to ensure that the termination will not be in violation of applicable law.
- Consider a progressive discipline policy first before termination.
- Conduct the firing in a dignified manner and in front of a witness, away from other employees.
- Be brief, accurate, respectful, and truthful about the termination.
- Make sure all legal requirements are fulfilled, such as having the employee's last paycheck ready together with any accrued but unpaid PTO.
- If you are going to offer a severance package, make sure you get a complete and full release from the employee (the release should be in writing signed by the employee, cover all known and unknown claims the employee may have, and be supported by adequate consideration). Note that special rules for releases may apply if the employee is 40 years old or older.
- Make sure that the employee's access to your computer network, voicemail, and email will be revoked upon termination.
- Ask for the return of any company laptops, phones, keys, security fobs, and the like.
- Make sure the employee has the information necessary to obtain COBRA (Consolidated Omnibus Budget Reconciliation Act) and unemployment benefits.
- Make sure the employee understands that she will have continuing obligations under any Confidentiality and Invention Assignment Agreement.
- Have the terminated employee leave the premises immediately, but give them an opportunity to pack up their personal belongings privately and discreetly.
- In anticipation that there may be litigation, make sure that all relevant emails and other documents concerning the employee are preserved.
- Make a plan for how the terminated employee's workload will be picked up by team members. That may also require a debriefing with the team, but be sure to protect the privacy of the departed employee.

5. EMPLOYEE PARTICIPATION PROGRAMS: UNITED STATES VS. GERMANY



When German technology companies want to hire qualified and talent members to their team in the United States, they will often find that they may need to offer adequate compensation systems to retain those individuals. In the United States this means some form of an employee participation program (be it equity-based or virtual). It should be noted that especially in Silicon Valley, not only employees but also many advisors will often request stock options and other equity interests, or, although rather uncommon in the United States, virtual shares.

EQUITY-BASED ESOPS IN THE UNITED STATES AND VIRTUAL VSOPS IN GERMANY

In the United States, employee participation programs are often set up as "real," *i.e.* equity-based, stock option plans/ESOP. A stock option gives a beneficiary the right to buy stock at a specified exercise price (or "strike price"). The beneficiary pays the exercise price and then receives the company stock. Under U.S. tax law, there are two types of stock options: (i) "incentive stock options" or "ISOs," and (ii) "nonqualified stock options" or "NQSOs." ISOs must meet substantial requirements to qualify for tax benefits to the employee. Nonqualified stock options can have more flexible terms but do not deliver as many tax benefits to beneficiaries but are subject to less stringent requirements. With each type of option, if the applicable requirements are met, there is generally no tax event on the date the option is granted, neither for the company nor the beneficiary. The tax treatment of the two types of options differs at the time of exercise of the option, and also during the period that the beneficiary holds the stock after it is transferred to her.

In Germany, similar equity-based ESOPs are rather unusual for a German technology company that has been set up as a GmbH (or, for that matter, an UG (haftungsbeschränkt)). The main problems with an equity-based ESOP in Germany are:

- Having many beneficiaries in the company's cap table is problematic because in a German GmbH, every shareholder has certain unalienable rights, including information rights or the right to challenge resolutions adopted by the shareholders' meeting.

- Shares and options in a German GmbH are not freely transferable as such transfers require notarization in front of a notary in Germany and, in most cases, a consent by the shareholders' meeting, a rather burdensome and costly process in particular when there are more than a few selected beneficiaries.

Thus, virtual employee participation programs ("VSOP") are much more frequent in Germany. VSOPs are designed to operate in a manner similar to an equity-based ESOP, but without delivery of actual shares or options. Rather, the beneficiaries obtain contractual claims (so-called "virtual shares" or "virtual options") against the issuing company for a cash payment in case of a liquidity event if the liquidity event and other circumstances satisfy the terms of the plan. As with an actual stock option, the value of the cash-out for the virtual option would be based on the liquidity event value of the company's stock. VSOPs can potentially deliver similar payout value to beneficiaries as equity-based ESOPs without invoking the limitations associated with such ESOPs (although VSOP payouts can be subject to higher US tax rates than are imposed on cash-out payments for stock acquired upon exercise of an option).

GERMAN VSOPS FOR U.S. BENEFICIARIES

To accommodate the expectation of their U.S. employees and advisors, German technology companies have the following options:

- If they flip into a U.S. company (see Chapter A.2 above), they can set up a typical U.S.-style ESOP on the level of the new U.S. holding company; or
- They can try to make an existing German market VSOP available to beneficiaries in the United States.

In fact, there are a number of advantages to using a virtual stock option program in the United States. First, the issuing company is not limited by tax regulations in terms of which service providers may be granted stock options. Please note that to address issues under the "Section 409A rules" under U.S. tax law, a stock option typically can be granted only to employees and service providers of the company and certain subsidiaries. With virtual stock option grants, those limitations do not apply and the company is able to grant stock options to service providers on the basis of its business goals. With virtual options, the company is also not required to grant a virtual option that has a strike price that is at least equal to the "fair market value" of the stock, giving it more flexibility to set an appropriate strike price than it has with real stock options. However, German technology companies must be aware that in many cases typical German VSOPs are not compliant with U.S. law, in particular U.S. tax law. Applying them without proper amendment for beneficiaries that are subject to U.S. taxation can result in material tax liabilities and even criminal liability for the beneficiary.

In the United States VSOPs must comply with the "Section 409A rules," or must qualify for an exemption from those rules. The "Section 409A rules" can result in restrictions on the payout triggers, and can also limit flexibility to change the plan's terms in the future. Thus, it is advisable to adopt the German VSOP along with a special supplement for U.S. beneficiaries. The U.S. supplement will be annexed to the German VSOP, and that supplement will modify the VSOP and prevail in case of any conflicts with the main body of the VSOP for matters that involve U.S. beneficiaries. Here are a few examples for

provisions that are typical in German VSOPs and that would need to be amended in the U.S. supplement when extending the German VSOP to beneficiaries subject to U.S. taxation:

- Typical German VSOPs often provide for a suspension of the vesting period in case of a maternity/paternity leave, sabbatical, long-time illness, etc. For U.S. beneficiaries such an expansion may only apply to the extent permitted by applicable U.S. federal, state or local law with respect to the applicable leave or suspension of employment and only to the extent it would not change the intended tax treatment of VSOP grants.

- Typical German VSOP provisions regarding the definition of a "good leaver" and a "bad leaver" do not fit with U.S. employment concepts. Thus, such good leaver and bad leaver definitions must be amended as well, *e.g.*, in many cases with respect to the definition of "cause" for the termination of an employment contract that would render a U.S. beneficiary a "bad leaver."

- Typical German VSOPs with respect to the payout of the beneficiary's claims in case of a liquidity event need to be amended as well. For example, a U.S. participant may benefit from payments relating to deferred payments, escrow amounts or earn-outs agreed upon in the contracts underlying the liquidity event only if such payments are made pursuant to payment and timing structures that comply with (or are exempt from) rigid U.S. tax laws under the Section 409A regime.

6. MANAGING LITIGATION RISKS

When contemplating entrance to the U.S. market, newcomers are often worried about the increased liability exposure. The litigation risk in the United States is indeed significantly higher than in many other countries. Customers and employees are more likely to resort to litigation than their German peers. Then there are also the infamous "patent trolls," whose business model consists in buying up patents and then seeking license fees from companies whom they claim are infringing those patents.

HIGHER LITIGATION RISKS IN THE U.S. MARKET

There are several factors contributing to the much higher litigation risks in the U.S. market:

- One of the main reasons is that filing lawsuits is rather inexpensive. Court filing fees are comparatively low and attorneys are often willing to agree to contingency fees, where the fees are payable only if there is a favorable result for the plaintiff. The "loser pays" rule does not apply in U.S. litigation, so each party typically pays its own attorneys' fees and legal costs regardless of which party prevails. Consequently, as plaintiffs do not bear the risk of paying attorney's fees and legal costs of the defendant, the hurdle for potential plaintiffs to assert claims is pretty low.
- U.S. litigation allows for a very liberal pretrial discovery. During this rather early phase of the litigation, the parties have to make available to the other side all evidence in their control that may be relevant for the outcome of the case, including evidence which is detrimental to the disclosing party's case – something that is unthinkable in civil law jurisdictions such as Germany. Discovery, and particularly e-Discovery, is very burdensome; sometimes thousands of documents are exchanged. The time and cost expenditure associated with pre-trial discovery will make many defendants accept a (cheaper) settlement even when faced with a weak claim.

- Where the case is tried by a jury of lay people (instead of trained professional judges) – a right granted to all litigants by the U.S. constitution – the outcome of the case is somewhat more unpredictable as is the amount of damage that is potentially awarded to the plaintiff. This holds particularly true for product liability cases.
- Another factor that makes U.S. litigation more risky is the possibility of "class actions." This special instrument allows suing a defendant on behalf of a great number of persons (for instance consumers) at the same time, who claim to have been harmed in the same or in a similar way. This instrument is particularly helpful for plaintiffs with small claims who would not have litigated individually.
- Defendants in the United States also face the risk of being ordered to pay "punitive damages," which might be substantially higher compared to granted damages in civil law jurisdictions such as Germany. Punitive damages are widely applied in the field of product liability. They go beyond the compensation of actual (material or immaterial) losses and aim at punishing the defendant as well as setting a deterrent example to other individuals or companies.

FIVE MITIGATION TOOLS TO LIMIT LITIGATION RISKS

In order to reduce litigation risk, participants in the U.S. market should consider, *inter alia*, the following strategies:

- **Corporate Structuring of the Business:** It is not advisable to operate in the United States through a U.S. branch of the German technology company, but rather to set up a U.S. corporation. The use of a branch directly subjects the entire assets of the German technology company to U.S. liability risks, while a separate U.S. corporation offers a liability shield. Even when doing a Flip of the German company into a U.S. company, in many cases, it is also worth considering setting up a second U.S. corporation as an operational subsidiary of the new U.S. holding company to shield the holding company's shares in the German technology company from U.S. liability risks.

HOW TO REDUCE THE RISK OF *"PIERCING THE CORPORATE VEIL"*

As a general rule, a U.S. corporation shields its shareholders from liability for the corporation's actions and omissions. However, there are certain exceptions. Most importantly, under U.S. law a court will "*pierce the corporate veil*" and hold a parent company liable for the actions of the corporation, if the parent exercises so much control over the subsidiary that the latter is a "*mere instrumentality*" of the parent. Hence, particular importance should be paid to ensuring that the subsidiary is sufficiently independent. A selection of factors that should be considered include:

- The subsidiary is adequately capitalized.
- Parent and subsidiary comply with corporate formalities.
- The subsidiary exercises business discretion.
- There is little or no overlap of officers or directors of parent and subsidiary.
- The parent deals with the subsidiary at arm's length.
- Property and financials of parent and subsidiary are clearly separated.

- **Contracts:** U.S. contracts tend to be much longer and more detailed than contracts for similar purposes in the German market. Advised by qualified legal counsel, companies go to great lengths to draft their contracts in a tailored way to minimize litigation risks. In particular, all contracts should clearly describe service and performance obligations, and they should specify limitations of liability. For details regarding employment agreements, please see above under Chapter B.4.

- **Compliance:** It is advisable to establish a dedicated compliance function. Companies should have at least one compliance officer responsible for ensuring compliance with contracts, laws and regulations, in particular regarding the areas of tax and regulatory issues.

- **Insurance:** It is absolutely crucial to carefully review whether the company's existing insurance protection is adequate for the litigation risks in the U.S. market and, where needed, to obtain additional coverage. In addition, U.S. regulations may require certain mandatory insurance policies (such as workers compensation insurance for employees), other policies might be required by U.S. contractual counterparties (such as professional liability insurance, certain kinds of automobile coverage, etc.). Other insurance policies might not be required by law or contract but are nevertheless highly recommended, in particular adequate D&O insurance coverage should be obtained in almost all cases. Depending on the company's business model an IP liability insurance or a policy against the fallouts of a cybersecurity breach might also be good ideas.
- **Pro-Active Management and an Awareness Culture:** Companies must educate their leadership teams and install adequate monitoring and reporting processes to identify potential problems early on, especially in HR matters, which should always be handled sensitively. In order to avoid punitive damages in product liability cases, which presuppose an intentional or exceptional gross negligent behavior, it is important to watch for indications for product, construction and instruction errors and to take timely measures like recalls.

A CLOSER LOOK:

CYBER INSURANCE – A NEW COVERAGE TO ENHANCE IT SECURITY POSTURE

Cyber insurance has reached a tipping point. The rising costs faced by data breach victims, which can exceed USD 100 million for the largest breaches, have spurred an increasing number of companies across industries to turn to cyber insurance in an effort to transfer at least some of those costs to an insurer. But cyber insurance is still relatively new, at least as a mass-market insurance product, and it is evolving quickly, although not as quickly as the threat itself. The policies are complex and not standardized, and courts have yet to provide any guidance about what will be covered and what will not. This state of affairs leaves many companies that have or are considering buying cyber insurance uncertain – not only whether they will be a victim of a data breach but also whether insurance will provide them with the coverage they need if they do become a victim. For a cutting edge overview of this rapidly evolving field and the key coverage and exclusion battlegrounds see our article **"Cyber Insurance: An Overview of an Evolving Coverage"** at our blog **"Trust Anchor – Current Trends in Cyber Security, Data Privacy and Regulatory Compliance"** at: http://blogs.orrick.com/trustanchor/.

7. AN INCREASINGLY IMPORTANT AREA TO WATCH: CYBERSECURITY AND ITS REGULATION

A more frequent area of scrutiny in assessing investment risk (not only in the M&A arena but also for larger VC financing rounds) is the a company's cybersecurity posture, both in terms of the cyber threats it faces and whether it is appropriately mitigating those risks. In response to an exponential increase in the volume and destructiveness of cyber incidents, U.S.-based companies are subject to a correspondingly large number of laws, regulations, enforcement actions, and standards intended to combat the risks posed by cyber-attacks. This surge in activity, from both federal and state regulators, has resulted in a de facto set of security compliance requirements organizations are expected to comply with to protect employees, consumers, investors, and the public at-large.

(YOUNG) TECHNOLOGY COMPANIES AS ATTRACTIVE TARGETS

Over the last twenty years, cyber threats evolved from what were initially perceived as acts of vandalism, petty crime, and trespass to far more lucrative criminal conspiracies focused on monetizing data and information through theft and extortion. Currently, the greatest risks companies are facing include highly destructive and sophisticated attacks, primarily committed by nation-state actors, on critical networks, systems, applications and, more recently, products, which can result in significant operational disruptions and/or serious harm to public health and safety. Even with respect to information, attackers are using increasingly creative cyber techniques to steal sensitive proprietary information, commit insider trading, and manipulate information for benefit. Although the attacks may have become more complex and significant, the targets of such attacks are often smaller companies specifically because they do not have sufficient resources to protect their assets, but often have valuable, innovative proprietary technology or serve as vehicles for attackers to infiltrate larger, more lucrative organizations. In short, it is precisely those companies that present interesting investment opportunities that may also be attractive to malicious actors. Once attacked, many of these companies are either unaware that they've lost valuable assets or simply can't recover from the devastation.

DATA BREACH

No one wants to inherit a data breach or invest in a company whose valuable intellectual property or data has already been stolen. One need only look at Verizon's recent acquisition of Yahoo! to recognize the substantial impact an undisclosed cyber incident can have on value. Understanding the security risks of your investment target is essential for early mitigation of those risks, and assessing the legal, financial, and reputational exposure they create.

In reaction to these threats, both U.S. federal and state regulators have started placing increasingly prescriptive requirements on companies to protect both information and systems from cyber threats. Regulatory expectations regarding internal security practices have been promulgated through laws, regulations, enforcement actions, standards, and guidance document. Penalties and damages for non-compliance can easily run into the millions of dollars following a data breach or significant cybersecurity incident, in addition to the reputational damage and loss of business suffered by a company following an incident. Moreover, larger companies are pushing down these requirements to vendors, service providers, and suppliers through contract provisions.

As discussed more fully below, the risks to companies vary across industry sector and services, and there is no one-size-fits-all solution; accordingly, it often behooves founders and investors alike to consider the appropriateness of a company's security practices in light of the potential cyber threats and liability associated with the company's industry sector, products and services, including its handling of personal data, and the resources available to secure its assets. In some cases investors may want to ask for specific vulnerability assessments and testing to identify current risks; an even more aggressive approach is to demand the performance of scans to uncover evidence of a prior hack of the target's network and systems.

REGULATORY COMMON LAW

Regulation in this area has largely developed from enforcement actions brought by federal agencies following notice of a data breach. This after-the-fact review and assessment of the steps that companies took to protect consumers' information has resulted in a sort of "common law" body of expectations as to what constitutes a "reasonable" security program by a company collecting, processing, or otherwise handling consumer data.

The Federal Trade Commission ("FTC") has been on the forefront of these developments. Relying on § 5 of the FTC Act, the FTC has regulated inadequate security practices pursuant to its authority to regulate "unfair or deceptive acts or practices in or affecting commerce." (15 U.S.C. §45). Based on the body of settlement orders entered into by the FTC and regulated companies, a "reasonable" security program to protect consumer data would include, at a minimum:

- Executive and board of director oversight over security risk management, including adequate funding/resources;
- Regular risk assessments;
- Adequate security controls and tools to monitor, detect, and prevent security incidents (e.g., anti-virus, encryption, access controls, patching programs);
- Employee awareness and training;
- Documented security policies and implementation and enforcement of those policies;
- Incident response preparedness and planning, including exercises;
- Effective remediation of vulnerabilities; and
- Third-party management of vendors, partners, and the supply chain).

Moreover, since its initial focus on post-breach scrutiny of internal corporate network security practices, the FTC has expanded its inquiry into security practices in other contexts, including but not limited to, application and software development, Cloud services, and the Internet of Things (i.e., product development). In addition to enforcement actions in these other areas, the FTC publishes frequent guidelines to communicate its expectations to commercial businesses.

Although this established common law provides some guidance for developing a compliant security program, historically, precise technical security requirements have not been mandated and are subject to an organization's own assessment of its particular risk profile.

SECTOR SPECIFIC REGULATORY REQUIREMENTS

In addition to the FTC, several other federal agencies have promulgated cybersecurity-related regulations and guidelines governing the industries they oversee. Such sector-specific cybersecurity rules include, for example: the Gramm-Leach-Bliley Safeguards Rule, which applies to financial institutions' protection of customer financial data, and the New York Department of Financial Services Cybersecurity Rule, which focuses on the security of the networks and systems of financial institutions' licensed in New York; the Federal Drug Administration's Pre- and Post-Market Guidance on Management of Cybersecurity in Connected Medical Devices, and the Health Insurance Portability and Accountability Act Security Rule governing patient health information; and multiple laws and standards applicable to businesses in other critical infrastructure sectors including, for example, transportation, energy, and communications, as well as particularly prescriptive requirements for U.S. federal government contractors.

The Securities & Exchange Commission ("SEC"), which has primary responsibility for regulating the securities industry and enforcing U.S. securities laws, has been increasingly active in the area of cybersecurity as well. In February 2018, the SEC promulgated a Cybersecurity Guidance document outlining its expectation for companies on issues such as (1) disclosing cybersecurity incidents in financial statements; (2) correcting prior disclosures; (3) selective disclosure of cybersecurity incidents; and (4) criteria for instituting trading black outs after discovering an incident. Based on recent SEC enforcement actions, and the April 2018 settlement order with Yahoo! in particular, we can expect a lot more SEC activity in this area in the coming years.

RELIANCE ON STANDARDS TO ASSESS SECURITY

Because of the uncertainty regarding what constitutes "reasonable" security (particularly since the threats and technology continue to change and evolve), industry associations and regulators also look to the expanding body of standards published by standards-setting bodies.

Perhaps the seminal document used by organizations to develop and assess sound security programs is the National Institute of Standards and Technology ("NIST") "Cybersecurity Framework." In 2013, President Obama issued Executive Order 13636 ("EO") entitled "Improving Critical Infrastructure Protection" to address the increasingly serious national security concerns posed by cyber threats against the country's critical infrastructure. As mandated by the EO, NIST was directed to lead the development of a framework to reduce cyber risks to critical infrastructure. That effort resulted in the publication of the NIST Cybersecurity Framework in February 2014 to provide a voluntary framework for companies who maintain or support the country's critical infrastructure networks to assess and improve their ability to prevent, detect, and respond to cyber-attacks. Although initially focused on core critical infrastructure protection, the Cybersecurity Framework establishes a common terminology and set of core security functions that companies across industries now use to manage cybersecurity risk.

In addition to the Cybersecurity Framework NIST has published a series of detailed standards and guidance documents covering a wide-variety of security topics for maintaining appropriate safeguards and processes (NIST 800-53, in particular, is a comprehensive set of security controls that are useful for program development). In addition, the Center for Internet Security published the twenty Critical Security Controls, a concise list of common technical controls; in addition, ISO 27001/27002 standards are still in use, particularly outside of the U.S.

Moreover, various industry sectors have developed their own standards including, for example, the Payment Card Industry Data Security Standard (PCI DSS); the Critical Infrastructure Protection (CIP) Cyber Security Reliability Standards promulgated by the North American Electric Reliability Corporation; and the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool, to name a few.

STATE LAW

U.S. states are also expecting more in terms of cybersecurity from companies doing business in their states. All fifty states now have data breach notification laws requiring notice to consumers whose personal data has been compromised. Those notifications may also lead to further inquiry by state Attorneys General; specifically, most states have state consumer protection laws (so-called "mini-FTC Acts") to address unfair or deceptive practices pursuant to which state Attorneys General will initiate inquiries about security practices. Moreover, roughly a dozen states have enacted state laws establishing specific minimum data security requirements to protect consumer data (e.g., Nevada, New Hampshire, Massachusetts).

California has been on the forefront of these developments. In 2016, the Office of the Attorney General for California declared (in an annual publication named the California Data Breach Report) that a failure to implement the twenty CIS Critical Security Controls applicable to an organization's environment "constitutes a lack of reasonable security." More recently, the California legislature passed the California Consumer Privacy Act of 2018 which establishes a private right of action following a security breach based on an alleged failure by the company to satisfy reasonable security measures. The law applies to all companies – foreign and domestic – who collect, sell, buy, or otherwise share the personal data of California consumers, and meet other specified threshold requirements.

CONTRACTUAL REQUIREMENTS

As noted previously, vendor management is a core component of a sound cybersecurity program, and is mandated by several of the laws and standards noted above. Generally vendor management encourages companies to contractually push down regulatory requirements and applicable standards to the vendors, suppliers, service providers, and other third parties with whom they engage. This is particular true for out-sourced vendors that process personal data or perform IT administrative and support functions that entail access to company networks. The contractual requirements can come in several forms: delivery of applicable certifications (e.g., PCI DSS certification); a general requirement to have "reasonable" security; obligations to satisfy contractually-specified security controls or RFP requirements; or obligations to comply with particular standards.

In addition to the technical and programmatic security obligations (often in the form of a contract addendum), commercial contracts more frequently include standard provisions that include specific security-related requirements, including, but not limited to, specific representations and warranties; incident notification obligations; limitations on liability; indemnification; audit rights; and insurance requirements.

IN SHORT, there appears to be no end in sight to federal agency activity and promulgation of increasingly prescriptive mandates to respond to the risks posed by new and significant cyber threats. Accordingly, founders and investors should include a review of a target's cybersecurity compliance as part of their routine due diligence. Such diligence requires a full understanding of a company's particular security threat profile and the regulatory expectations and best practices most appropriate to the particular industry or ecosystem in which it operates.

OUR INTERNATIONAL PLATFORM FOR TECHNOLOGY COMPANIES

Dedicated to the needs of technology companies and their investors

Orrick counsels more than 1,800 tech companies as well as the most active funds, corporate venture investors and public tech companies worldwide. Our focus is on helping disruptive companies tap into innovative legal solutions.

We are a top 10 law firm for global M&A volume (*MergerMarket*) and the #1 most active law firm in European venture capital, and M&A exits (*PitchBook*).

Oracle | Microsoft | NVIDIA Intel | Cisco | Pinterest | Stripe 23andme | eHarmony | SoFi Betterment | Planet Labs

JUVE NOMINIERT JUVE Awards 2017 Kanzlei des Jahres für Private Equity und Venture Capital

The leading German legal data base *Juve* nominated us for **Private Equity and Venture Capital Law Firm of the Year 2017** in Germany.

LAW360

Tech Group of the Year
2X
Law360

The LEGAL 500

Leader in Venture Capital and Corporate Practice
Legal 500

PitchBook

Most Active VC law firm in Europe
for ten consecutive quarters
PitchBook Q2 2018

THE STATE OF EUROPEAN TECH 2017

State of European Tech

The 2017 State of European Tech Report prepared by *Atomico* in collaboration with *Slush* and supported by Orrick and Silicon Valley Bank, is the latest evidence of Europe's growing influence in the global tech ecosystem.

FT FINANCIAL TIMES

Honored for Connecting the German Mittelstand with Start-ups

In its **2017 European Innovative Lawyers Report**, the *Financial Times* awarded our German Technology Team a top three position in the category of supporting start-ups and innovation. In this Europe-wide and in-depth research, the *Financial Times* labeled our corporate venture capital initiative led by Düsseldorf partner Sven Greulich as "*outstanding.*" In its reasoning, the *Financial Times* further stated: *"Connecting Germany's Mittelstand (mid-sized companies) with start-ups, the firm is tackling tax issues in stock option plans, making bridges between Silicon Valley and Germany, and showing the way for successful investments."*

A TRULY GLOBAL PLATFORM.

Nest
US$3.2 billion acquisition by Google
Seller's Counsel

Yammer
US$1.2 billion acquisition by Microsoft Corporation
Seller's Counsel

Instagram
US$1 billion acquisition by Facebook (U.S.)
Seller's Counsel

Cruise
Over US$1 billion acquisition by General Motors
Seller's Counsel

TOA Technologies
Acquisition by Oracle (terms not disclosed)
Seller's Counsel

AVG
US$1.3 billion acquisition by Avast
Seller's Counsel

Apple
Acquisition of WiFiSlam and Siri (terms not disclosed)
Acquiror's Counsel

Pinterest
Acquisitions of Kosei (terms not disclosed)
Acquiror's Counsel

WE ADVISE TECH COMPANIES AT ALL STAGES:

8 of the 10 largest Silicon Valley/SF Bay Area Companies by Market Capitalization

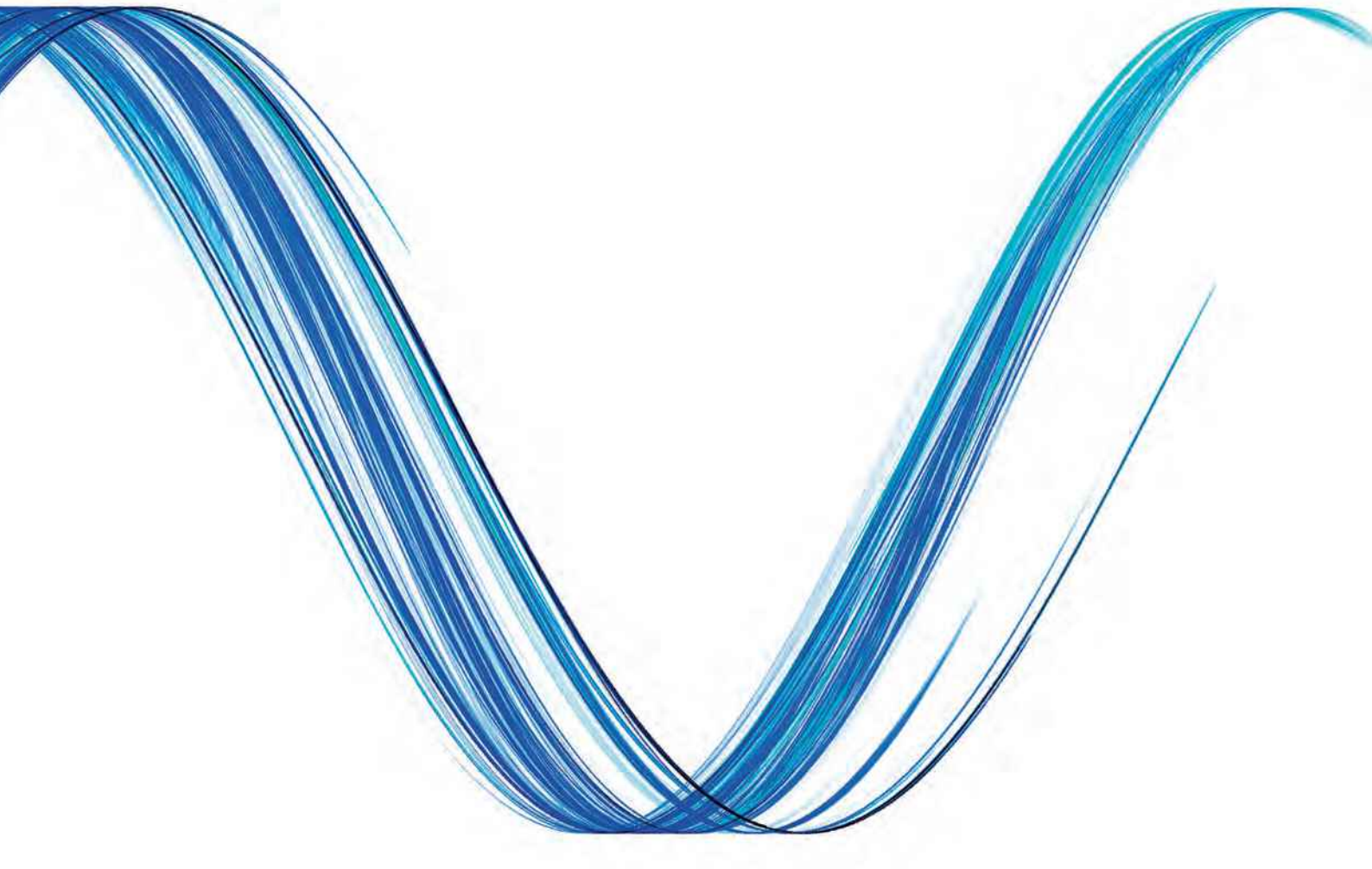
≈ 20% of all **US$ 1 Billion+ Unicorns** in the U.S. Market

6 of the **Fortune 10** TMT Companies

In 2017 alone, we advised on **650+** venture financings with a combined value of more than **US$ 12.4 billion** in **30** countries.

Operating in 25 markets worldwide, we offer holistic solutions for companies at all stages, executing strategic transactions but also protecting intellectual property, managing cybersecurity, leveraging data and resolving disputes. We are helping our clients navigate the regulatory challenges raised by new technologies such as crypto currencies, autonomous vehicles and drones. A leader in traditional finance, we work with the pioneers of marketplace lending.

We innovate not only in our legal advice but also in the way we deliver legal services, earning us the #1 spot on *Financial Times*' list of the most innovative North American law firms in both 2016 and 2017.



LEADING IN LEGAL INNOVATION

DELIVERING VALUE THROUGH LEGAL SERVICE INNOVATION

"What are you doing to innovate and enhance value?"
We hear this question from our clients every day. As a law firm focused on serving leaders in Technology & Innovation, Energy & Infrastructure and Finance, we are listening. And we are collaborating with clients to drive change.

THE IPO READINESS TOOL

Orrick and LTSE partnered to create a first-of-a-kind IPO readiness assessment tool. Whether you're a tech company getting ready to go public or an early-stage start-up, this tool and our related resources will provide insight into your company's health.
We designed this solution drawing on our experience counseling 1,800+ high-growth companies.

In just 20 minutes, the IPO assessment tool provides a stress-test on everything from your investment narrative and financial infrastructure to team strength and corporate governance. If a public offering is in your business plan, on LTSE or any exchange, this tool and the resources below can help set you on a path to success. For more information and to take the test go to: www.orrick.com/Practices/IPO-Ready.

#1 MOST INNOVATIVE LAW FIRM IN NORTH AMERICA 2016 & 2017 – *Financial Times*

Orrick partner Sven Greulich's work to connect start-ups with Germany's Mittelstand is a standout "for making bridges between Silicon Valley and Germany."
Financial Times Innovative Lawyers Report Europe

"**In the Bay Area**, law firms have a penchant for blurring the lines between themselves and the start-ups that surround them. The result is Orrick Labs, a small project under the Orrick roof that looks to build products that its lawyers need."
Above the Law

Orrick Analytics

ORRICK ANALYTICS

Orrick Analytics is a team of lawyers, statisticians and other professionals that uses state-of-the-art technology and probability modeling in document-heavy engagements. The type of work ranges from massive document reviews in litigation to large-scale contract reviews and other due diligence. The Analytics team's mission is straightforward: enhance speed and accuracy of document review; generate insights specific to the engagement; and reduce our clients' costs.
For more information see: www.orrick.com/Innovation/Orrick-Analytics.

ORRICK LABS
Powering Innovation

ORRICK LABS

We launched this skunkworks-style operation to accelerate the development of legal technology client service quality, security and efficiency.
A team of in-house technologists (including experts for cloud-based computing, artificial intelligence and data security) work closely with our lawyers in the field to turn their and our clients' ideas into reality.
For more information see: www.orrick.com/Innovation/Orrick-Labs.

ABOUT THE AUTHORS

ABOUT THE AUTHORS

CORPORATE AND FINANCE

Sven Greulich
(Author and Editor)
Düsseldorf
sgreulich@orrick.com

Sven Greulich advises technology companies on complex cross-border mergers and acquisitions, as well as private equity and venture capital investments. Sven is passionate about building a bridge for his clients from Germany to Silicon Valley and other global technology hubs. He is an alumni of WHU, Germany's top business school best known for its entrepreneurial focus where he is a frequent guest lecturer on venture capital law and supports various entrepreneurship initiatives. In the 2017 edition of its Innovative Lawyers Report Europe, the *Financial Times* named Sven's work to connect start-ups with Germany's Mittelstand (mid-sized companies) a standout *"for making bridges between Silicon Valley and Germany."* In 2017 and 2018 he received the Acritas Star Lawyer Award and is recommend by Chambers for mid-size international corporate M&A transactions.

Tal Hacohen
New York
thacohen@orrick.com

Tal Hacohen is a partner in the Corporate Group of Orrick's New York office and is a member of the Global Mergers & Acquisitions and Private Equity Group. Tal represents U.S. and multinational public and private company clients in a variety of transactions and across industries, including domestic and cross-border mergers, acquisitions, dispositions, private placements and restructurings. Tal also represents founders, companies and investors in venture capital financings, and advises boards of directors and shareholders in all aspects of New York and Delaware corporate, partnership and limited liability company law, including corporate governance and fiduciary duty matters. Tal was recently recognized as a "40 under 40 Emerging Leader" by The M&A Advisor, an "Acritas Star Lawyer" by Acritas and a "Rising Star" by IFLR for his work in the area of Mergers & Acquisitions.

Shawn Atkinson
London
satkinson@orrick.com

Shawn Atkinson is a member of the European Technology Companies Group who advises leading private equity, venture capital, growth funds and high-growth technology companies. He has a particular depth of experience in technology and IP-rich businesses and is a recognized leader in late-stage venture transactions and in early-stage private equity transactions in Europe and emerging markets. A cross-border transactional lawyer by trade, his experience includes U.K. multijurisdictional and complex corporate transactions for both public and private companies, including countless acquisitions and disposals, cross-border mergers, bankruptcy-infused asset sales, recapitalizations and reorganizations. Shawn has been a "*recommended individual for Venture Capital and Mid Market M&A*" by *Legal 500 U.K.* in each of the last four years.

John Bautista
San Francisco, Silicon Valley,
Santa Monica
jbautista@orrick.com

John Bautista is a member of Orrick's Board of Directors and Orrick's Technology Companies Group. He leads the international Technology Companies Group connecting Silicon Valley with Europe and Asia. John focuses his practice on advising emerging companies and investors, and represents both public and private high-tech companies in many areas, including corporate and securities law, venture capital financings, mergers and acquisitions, public offerings, public company representation, and technology licensing. He is recognized for his work with Y Combinator in helping to create the SAFE (Simple Agreement For Equity). In 2017, the *Financial Times* selected John as one of the *top 10 Most Innovative Individuals of the Year*.

Josh Pollick
Santa Monica
jpollick@orrick.com

Josh Pollick represents high-growth technology companies and venture capital firms in many areas, including corporate and securities law, corporate formations, venture capital financings, mergers and acquisitions, public offerings, secondary offerings and technology licensing. In addition to his company-side representations, Josh has represented leading venture capital firms and other strategic investors and has also helped set up a number of incubators and private funds, including Heavybit Industries and Velocity Group. He works with the USC Startup Garage and on a pro bono basis with the UC Hastings School of Law start-up clinic to oversee law students with formations of early-stage technology start-ups.

ABOUT THE AUTHORS

DATA PRIVACY AND IT/INTELLECTUAL PROPERTY RIGHTS

Christian Schröder
Düsseldorf
cschroeder@orrick.com

Christian Schröder is head of the German Data Privacy & IT/IP Group. Christian advises start-ups to large multinationals on IP, unfair and deceptive trade practices, e-commerce, IT and data privacy/data protection. Christian provides IT/IP advice in M&A transactions and advises on IP-focused joint ventures. As a core member of Orrick's global Cyber, Privacy and Data Technology practice group, Christian has also special focus on data privacy/data protection matters. In particular, Christian advises on a risk-based approach to privacy, on implementing databases and new software applications and, in particular, cloud-based solutions. Christian has commented, *inter alia*, on Chapter V of the new EU General Data Protection Regulation (International Data Transfers) in: Kühling/Buchner, DSGVO, 2018.

Beth M. Goldman
San Francisco
bgoldman@orrick.com

Beth Goldman is a member of the Intellectual Property Group. Her practice focuses on trademark and copyright law, licensing, Internet law and advertising clearance. She has been assisting clients in the selection and creation of brands, as well as their protection, for more than 20 years. Her experience includes worldwide prosecution and policing of trademarks, dispute resolution, UDRP proceedings and litigation before the Trademark Trial and Appeal Board. Beth has spoken on trade dress for the Practising Law Institute on intellectual property, and on domain name and other issues for the International Trademark Association. She has served on various INTA committees.

Jennifer Martin
Silicon Valley
jennifermartin@orrick.com

Jennifer Martin is a member of Orrick's Cyber, Privacy & Data Innovation Practice. She focuses on a range of cybersecurity projects for clients, including advising on cybersecurity program compliance and resiliency on an industry-by-industry basis; managing significant security incidents and providing cross-disciplinary incident response planning; drafting commercial contract terms and requirements for purchasers and vendors as part of managing cybersecurity risk; and conducting cybersecurity due diligence in M&A transactions. Jennifer's holistic, company-wide incident response planning and risk management counseling are informed by more than 18 years of handling significant cyber incidents from a variety of legal and technical perspectives. She has significant experience managing the response and investigation into sophisticated cybersecurity attacks impacting systems and information, including those attributable to nation-states, insider thefts of intellectual property, and data breaches of all sizes and significance. Jennifer's early work as a federal and local cybercrime prosecutor and policymaker within the DOJ's Computer Crime & Intellectual Property Section provides her with historical insight into the evolving threat landscape and the consequent law enforcement and regulatory responses. In addition, Jennifer served as director of cyber incident response and operations and lead in-house internal investigations counsel at Symantec, was a Managing Director of Stroz Friedberg, a global forensic consulting firm, and led her previous firm's west coast cybersecurity practice.

Peter D. Vogl
New York
pvogl@orrick.com

Peter Vogl is a member of the Intellectual Property Group focusing his work on trademark, copyright, and false advertising matters. He has more than 30 years of experience representing brand and rights owners and is one of the most well-known trademark lawyers in the country. His practice includes trademark counseling and portfolio management on behalf of multinational and domestic consumer products and services companies. In addition, Peter advises clients on trademark and copyright audits, securitizations, acquisitions and divestitures of intellectual property portfolios.

Amy van Zant
Silicon Valley
avanzant@orrick.com

Amy van Zant is a member of the Intellectual Property Group. Whether litigating a complex patent suit, or advising on a multi-faceted IP strategy, Amy incorporates an in-depth understanding of each client's business, employees and corporate strategy into her solutions. For her litigation practice, Amy's ability to distill the most complicated technology across an array of fields, including telecommunications, semiconductor manufacturing, renewable energy, cloud computing, and big data, into relatable, every day concepts that has made her successful in persuading judges and juries alike. Amy also provides comprehensive IP counseling on issues including trade secrets protection, employee departure investigations, freedom to operate analysis, licensing strategies, data privacy protection, and regulatory compliance. In addition to her IP work, Amy devotes significant time to her pro bono work. For more than a decade, she has assisted domestic violence victims, as well as led Orrick's Bay Area summer program that enables law clerks to be certified to argue in Family Court to obtain Temporary Restraining Orders for domestic violence clients.

Emily S. Tabatabai
Washington D.C.,
Houston
etabatabai@orrick.com

Emily S. Tabatabai is a partner and founding member of the Cyber, Privacy & Data Innovation practice, which was named Privacy Practice Group of the Year by Law360 in 2016 and is nationally ranked by the Legal 500 USA for Cyber Law, Data Protection and Privacy. She has been recognized by the Legal500 for her "extraordinary depth of knowledge in student data privacy matters," and by Chambers-USA as "an invaluable resource to have when it comes to data privacy and security." She advises clients on an array of Internet commerce matters, including data privacy and data security compliance and procedure, data breach response, online and mobile privacy, student data and EdTech privacy, behavioral advertising, sales and marketing, advertising and promotions, and social media. Emily has represented clients from start-ups to Fortune 500 companies in investigations before the Federal Trade Commission and State Attorneys' General, as well as in private litigation.

ABOUT THE AUTHORS

LABOR AND COMPENSATION

André Zimmermann
Düsseldorf
azimmermann@orrick.com

André Zimmermann is head of the German Employment Group. He advises German and international companies in all areas of individual and collective employment law. The main focus of André's practice includes employment aspects of M&A transactions, restructuring, outsourcing and headcount reduction, multijurisdictional and cross-border employment issues, service agreements of managing directors and board members, codetermination of employees at operation and board level, collective bargaining and negotiations with works councils, trade unions and litigation.

Lynne C. Hermle
Silicon Valley
lhermle@orrick.com

Lynne C. Hermle is a partner specializing in employment law who tries cases before juries and in arbitration for some of the world's leading software, media, Internet and other technology companies. She was the lead defense counsel for Kleiner Perkins Caufield and Byers in its successful defense of the gender discrimination claims alleged by Ellen Pao and has since led the defense in SpaceX in two jury trials. Lynne has handled hundreds of employment claims involving sexual harassment, discrimination, retaliation, and wrongful termination. In recognition of her successes, she has been inducted into the American College of Trial Lawyers and received the Daily Journal "California Lawyer of the Year" two years in a row as well as other awards for trial successes.

Michael D. Weil
San Francisco
mweil@orrick.com

Michael D. Weil is a partner specializing in employment law. He represents clients in high-stakes employment, trade secrets, and employee mobility litigation throughout the United States. Michael was recognized as a Rising Star in his field by Law360. Michael's practice focuses on matters involving trade secrets, restrictive covenants, employee mobility issues, Sarbanes-Oxley (SOX) whistleblower claims, wrongful termination and discrimination. He has also defended numerous wage-and-hour class actions and representative actions under state and federal laws, including claims for overtime, vacation, meal and rest break penalties, waiting-time penalties, and other alleged Labor Code violations. Michael counsels clients on a wide variety of employment and related corporate issues.

Mitch Pahl
New York
mpahl@orrick.com

Mitch Pahl is a member of the Compensation & Benefits Group. Mitch represents public companies, financial institutions, government institutions, private equity groups and high net-worth individuals in the areas of employee benefits and executive compensation. Mitch has particular expertise relating to ERISA fiduciary and private equity matters, M&A transactions, compensation and benefit plan compliance, and the special issues encountered in connection with globally mobile executives. Mitch is widely recognized for his work relating to global executive compensation matters. He is the co-author of the "Multinational Executives" chapter of the leading Executive Compensation treatise, one of the first widely circulated publications to cover the topic. He has worked with clients in Africa, Asia, Australia, Europe, and North, South and Central America.

ABOUT THE AUTHORS

LITIGATION

Nicholas Kessler
Düsseldorf
nkessler@orrick.com

Nicholas Kessler is a member of the International Arbitration Group. He focuses on national and international arbitration and complex litigation, predominantly with regard to post-M&A, restructuring and corporate law, antitrust damages, and particularly construction disputes. Nicholas has extensive experience with arbitral proceedings under the auspices of all of the major arbitral institutions and rules (*e.g.*, ICC, DIS, SCC, LCIA, UNCITRAL, ICSID, *ad hoc*). He also regularly advises on general commercial law matters such as product liability and distribution law. Nicholas is a visiting lecturer at the Universities of Münster, where he teaches international arbitration and mediation in the university's post-graduate program. He is also a visiting lecturer at the University of Düsseldorf for European and International Civil Procedure.

TAX

Stefan Schultes-Schnitzlein
Düsseldorf
sschnitzlein@orrick.com

Stefan Schultes-Schnitzlein is head of the German Tax Group. Stefan is both qualified as a German lawyer (*Rechtsanwalt*) and as a German tax adviser (*Steuerberater*). He advises industry clients, private equity funds and financial institutions on all sorts of German tax and accounting issues, usually with a transactional background. Stefan's focus is on corporate and real estate transactions, financings, refinancings and restructurings as well as on tax field audits and tax litigation in connection with any of the former. Stefan has advised several German start-ups on their flip to a U.S. holding company as part of larger venture capital financings.

HELPFUL SOURCES

Other Orrick Guides

On our Tech Transactions Germany website, www.orrick.com/Practices/Technology-Transactions-Germany, you will find all our Germany related Tech guides including the following:

Orrick's Guide to Venture Capital Deals in Germany
Orrick, Herrington & Sutcliffe, February 2018.
available at: www.orrick.com/Insights/2018/02/Orrick-Guide-to-Venture-Capital-Deals-in-Germany-2018-Edition

Corporate Venture Capital 2017 – Structures, Challenges & Success Factors
Orrick, Herrington & Sutcliffe, July 2017.
available in German and English at: www.orrick.com/Insights/2017/06/Corporate-Venture-Capital-2017

Orrick Blogs

Check out our renowned blogs with latest market insights and legal developments in the U.S. and globally
www.blogs.orrick.com

Books

Daniel Kahneman
Thinking, Fast and Slow
Penguin, 2012.

In this international bestseller, Nobel Prize winner Daniel Kahneman distils a lifetime of groundbreaking behavioral economics research into an encyclopedic yet lucid coverage of the heuristics and biases that influence our supposedly rational decision-making processes.

Brad Feld & Jason Mendelson
Venture Deals
3rd edition, John Wiley and Sons, 2016.

Although focused on U.S. start-ups and venture-capital deals, this "classic" is a must-read for each generation of new entrepreneurs. In addition to describing venture financings in detail, it provides context around the players, the deal dynamics and how venture capital funds work.

Mahendra Ramsinghani
The Business of Venture Capital
2nd edition, John Wiley and Sons, 2014.

Focused on the U.S. venture capital market but also valuable for German market players, it is a pretty comprehensive insight into venture capital investments seen from the investor's perspective with data, industry trends and insights from leading U.S. investors and their financial sponsors.

Noam Waterman
The Founder's Dilemmas – Anticipating and Avoiding the Pitfalls That Can Sink a Startup
Princeton University Press, 2013.

Though less comprehensive than the seminal book by Kahneman mentioned above, this book is a good read for entrepreneurs and very early-stage investors alike as it draws on the insights from behavioral economics when examining the most important decisions entrepreneurs will face: should they go it alone, or bring in cofounders, hires, and investors to help build the start-up?

INDEX

INDEX (CONT.)

R

S

T

V

orrick

Your contacts

Düsseldorf
Dr. Sven Greulich LL.M. EMBA
sgreulich@orrick.com

Orrick, Herrington & Sutcliffe LLP
Orrick-Haus
Heinrich-Heine-Allee 12
40213 Düsseldorf

T: +49 211 3678 7261
M: +49 175 227 0012

Munich
Dr. Thomas Schmid
tschmid@orrick.com

Orrick, Herrington & Sutcliffe LLP
Rosental 4
80331 Munich

T: +49 89 383 9800

www.orrick.de