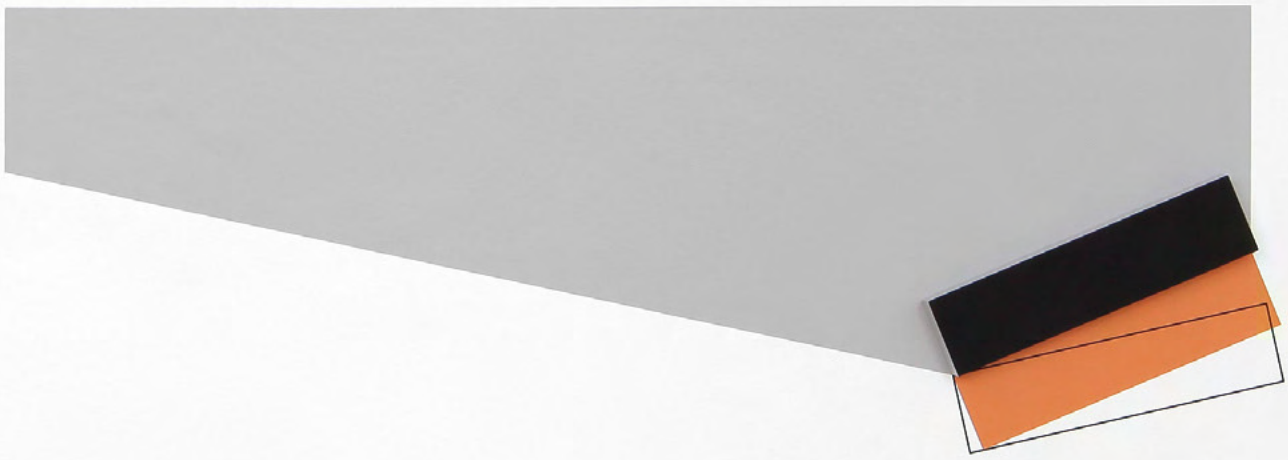
roadmap18



schönherr

privacy

Since being launched in 2007, the annual Schoenherr roadmap has highlighted significant legal developments in our markets, presenting them in a special context created in partnership with a different artist each year. This year we are pleased to present Manfred Makra as our collaborating artist.

With data privacy, among others being in the spotlight, the topic of this year's roadmap is privacy.

Our lawyers across CEE provide you with insight into legal privacy-related topics, applicable to each practice group throughout the region. This year we also highlight highly regarded external experts who give their views on thought provoking topics. We hope that you find our 2018 roadmap both interesting and enlightening.

Michael Lagler
Schoenherr Managing Partner

We are proud to present the 2018 Schoenherr roadmap. This year we focus on the general theme of privacy, and provide you with a 360-degree view of interesting and up-to-date aspects of the law across CEE. We again intertwine art which we feel fits in with the theme and adds aesthetic value to the publication.

The topics covered by our lawyers include among others: Banking Secrecy, Data Ownership, Confidentiality in Restructurings, Trade Secrets, Tax Secrecy vs Exchange of Tax Information, Criminal Procedural Law vs Individual Privacy / Liberty, and Data Privacy.

Our take on privacy is a blend of three elements:

the personal element of restricting others from gaining insight into one's personal matters, or the idea of physically being apart from others;

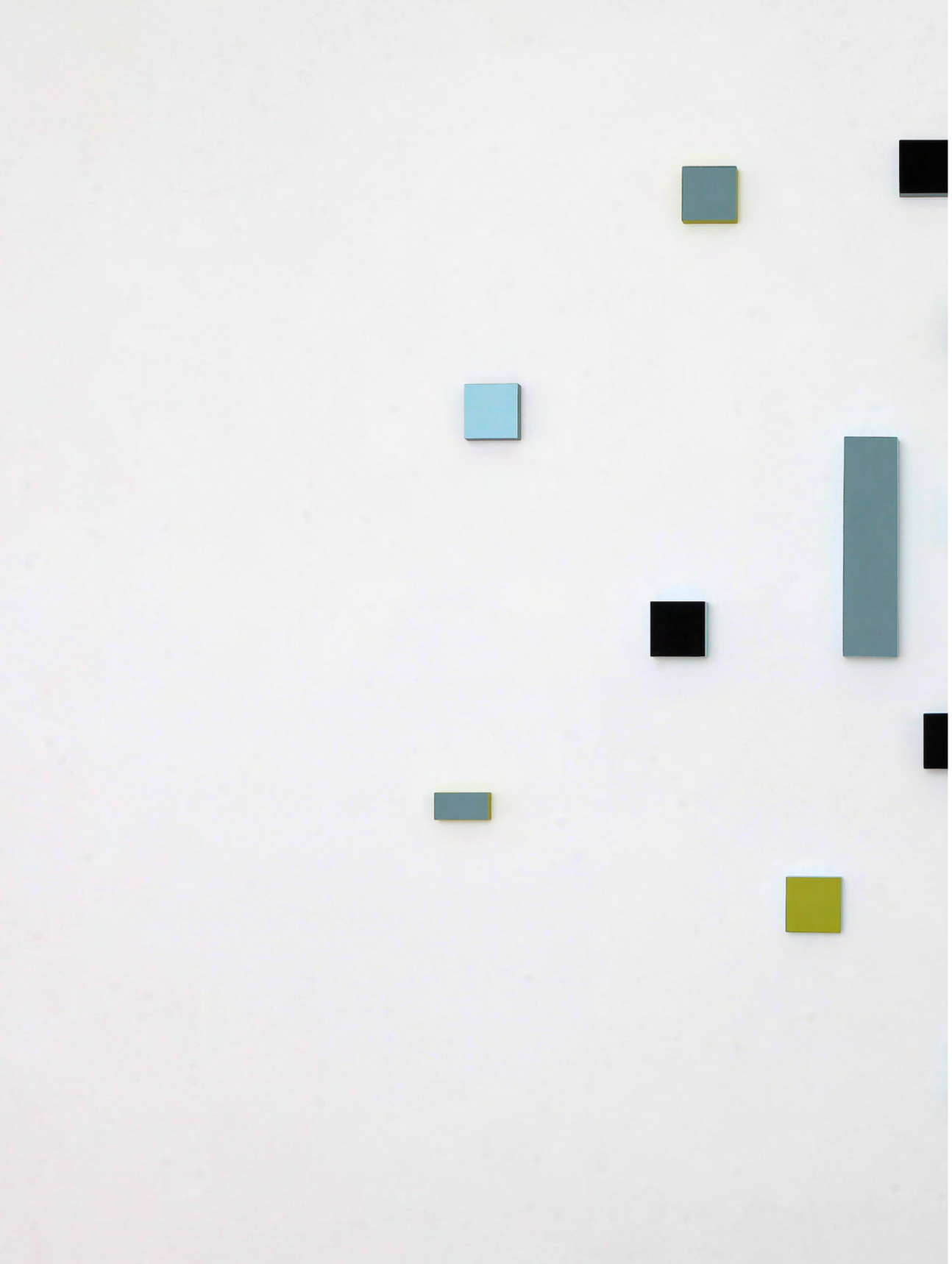
the legal context in which, very broadly speaking, the access to or the use of personally identifiable information is regulated; and

the artistic perspective, where the creation of art is a very private experience, and according to our roadmap18 artist Manfred Makra, "art is the bridge from the privacy of the artist to the privacy of the beholder."

Enjoy! We hope these legal snapshots accompany you through 2018, giving you fresh perspectives which are straight to the point.

Manfred Makra's interpretation of artistic privacy *vis a vis* privacy in a more general / personal sense, is highlighted in our artist feature later in this publication.
See pages 122 to 126

table of contents



01 banking, finance & capital markets

Banking Secrecy

Secrecy and portfolio transactions. A journey that doesn´t end with closing the deal

An interview by Martin Ebner | Laurenz Schwitzer

Banking secrecy still appears to be a dominant risk factor in regard to loan sale transactions. Whereas market practice exists for the implementation of a loan sale transaction, servicers may often not be aware of the potential impact and may still struggle to stay compliant troughout the serving period.

We reached out to Karel Smerak, the director of the secured NPL business in CEE/SEE for EOS (one of the key players in the region), to discuss how banking secrecy is affecting day to day work and how servicers can stay compliant.

Q: Karel, EOS is one of the leading non-performing loan servicers in the region with over 7,000 employees and active in more than 20 countries worldwide. As a director for NPL transactions in CEE, you oversee EOS's secured debt activities in the region. What keeps you busy these days?
A: Indeed, EOS evolved as part of the German company Otto Versand into one of Europe's leading servicers and investors in NPLs, with balance sheet assets of about EUR 1.5 billion. As for our regional footprint, we are basically active in three big regions: Germany as the home market, Western Europe (with a particular focus on France and Spain) and Central, Eastern and South Eastern Europe, which for us includes also Greece.

Historically, EOS has developed from the unit in charge of collecting unpaid debts from ordered goods from the Otto mail order catalogue in the 1970s, to the data-driven, full service dis-

banking, finance & capital markets **01**

> Banking secrecy appears to still be a dominant risk factor in regard to implementing loan sale transactions and the subsequent servicing of the loans.

tressed-debt investor and servicer that it is today. We currently cover all asset classes within the NPL space, from unsecured receivables to secured consumer mortgage loans to secured commercial loan portfolios.

We have seen EOS successfully participating in some of the recent secured / mortgage-backed NPL transactions in the region. What is your strategy with these assets? Would you say that those loans are rather collected by court enforcement, piecemeal sales / single tickets or sales in bulk, as smaller more targeted or bespoke portfolios?
It depends a little on which assets we are talking about. For consumer debt, we would usually first aim to reach a consensual deal in cooperation with the borrower. Typically this achieves the highest cash flow in the shortest period of time, and for the borrower it is the easiest way to resolve their situation.

Unfortunately, many borrowers stop communicating and don't even try to work with us, sort of hoping that at some point the problem will disappear. In this case we need to look at the legal possibilities available.

If we look at the corporate NPL portfolios that we are servicing in the region, they generally comprise bigger real estate-secured tickets. This means a more professional market, a more professional counterparty and a somewhat different legal landscape compared to private loans. For each of these larger corporate loans we develop alternative resolution scenarios, and decide for each individual case on the best strategy.

Just like with private debtors, we try to work with the corporate borrowers too, to find a consensual solution whenever this is possible. If the borrower isn't cooperating, or if a voluntary sale of the mortgaged real estate is not an option for other reasons, we have to go through a legal enforcement or bankruptcy process with a court-sponsored sale of the underlying asset, depending on the legal framework available. In specific situations we may consider a sale of a single receivable or of the entire exposure against a single corporate client to a specialised investor. With regard to potential onsale of smaller, “bespoke” portfolios, I have not come across many of these in the CEE region and it is not something you would typically see in the market.

Is taking over the ownership of the real property in the auction a strategy you would use to resolve a non-performing loan?
At EOS, if we have the choice we generally prefer not to become the owners of the underlying real property. Having said that, sometimes this is the best or in fact the only way to protect the value of the asset in an auction or resolve a complex legal impasse, and in those cases we are generally ready to step into the ownership title.

How does the issue of secrecy affect your work as the servicer of non-performing loans?
At EOS we are highly committed to staying compliant with all applicable laws and regulations. And secrecy laws – most of all banking secrecy and personal data protection – are an important part of the legal framework that we strive to comply with. Sometimes these banking secrecy or personal data protection laws may even negatively impact the recovery we are able to achieve, as the recovery often depends on how much information can be shared with a potential investor or – like in Hungary – how proactively a property can be marketed for sale. However, we

Karel Smerak is director of the secured NPL business in CEE / SEE for EOS, an Otto Group company and one of Europe’s leading NPL investors and servicers. He oversees the group’s transaction activity and servicing teams in the secured NPL space in the CEE / SEE region.

have made the decision that compliance always comes first, and whatever we do has to be done one hundred percent in line with the law. So your question is very relevant – secrecy legislation in the widest sense has an impact on us and is an important factor driving our resolution strategy for our cases.

Banking secrecy seems to still be a dominant risk factor in regard to implementing loan sale transactions and the subsequent servicing of the loans, despite the regulatory measures implemented to encourage banks to divest their nonperforming assets. Do you agree that the rather stringent Austrian banking secrecy regime may still give market participants headaches?
With respect to secrecy regimes that apply under Austrian law, I feel that there is still a kind of clash of two principles: banking secrecy and data protection vs allowing transactions to happen. Over-emphasising one principle may make a transaction *de facto* impossible.

I think that over time the market has found practical solutions on how to make a portfolio transaction possible, for example, via a staged access to certain types of information as you progress in the transaction or the “red room” concept, with certain information being accessible only to the investor’s professional advisors and not to the investor directly. Even if this means a rather slow-moving transaction process from the buyer's perspective, having a kind of generally accepted market practice helps getting the deal done.

However, once a portfolio has been acquired and servicers need to start recovering the loans, I think there is a wider range of awareness levels of different market participants. In particular for multi-jurisdictional portfolios it is likely that some of the less experienced servicers, if not part of the transaction as such, have never even heard that Austrian banking secrecy law could actually be applicable to parts of their portfolio that they service outside of Austria. This is also due to the fact that transaction lawyers usually stop being involved after a transaction closes, and the workout lawyers working on resolving a claim typically only look at local laws and might not even be in a position to assess whether and what secrecy regimes apply. On a practical level, the issue of banking secrecy often materialises when more detailed

> Servicers still seem unaware that compliance regarding banking secrecy and data protection actually becomes even trickier once servicing has commenced.

information needs to be disclosed by the servicer during day-to-day business, for example when the servicer is negotiating the sale of a single ticket to a potential investor. We at EOS are well aware of the Austrian banking secrecy issues inherently present in this situation, but I suspect that this may not be the case for all the other servicers, which enhances the probability that secrecy laws are not being complied with.

How are you – and EOS more generally – trying to cope with these challenges as a servicer? What does proper compliance in respect to banking and data secrecy mean to you?
I think that as an international servicer, who is also often involved in portfolio transactions as an investor, we have the advantage of being aware of the challenges that lie ahead during the servicing period and that are present within the various legal systems. This allows us from the very start to put compliance with banking secrecy and personal data protection high on the agenda and to ensure that the relevant knowledge is being transferred from the transaction team to the case managers.

For us, proper compliance first of all means that we comply 100% with the law, even if this may mean that we cannot fully pursue our economic interest. One of the instruments to achieve full compliance is implementing stringent compliance procedures on every level in each jurisdiction.

I'll give you an example from Croatia, where we worked with our lawyers to develop an in-house policy and a documented process on how we deal with loans that may be affected by Austrian banking secrecy laws. This process helped case managers form a view as to how to identify potentially affected loans, to define the admissible actions that can be pursued and which information can be disclosed.

Our cooperation not only included staff training, but also measures to ensure that these guidelines are practically implemented. We have taken the same approach also in other situations with regard to banking secrecy.

It's one thing to have guidelines on paper, but it's more important to make sure that they are followed in practice, which starts with involving the employees in drafting these guidelines, through relevant training provided periodically, also when new staff joins the team, and including ad hoc checks, just to make sure that the process has actually been complied with. So far it has been working out quite well.

Servicers still seem unaware that compliance regarding banking secrecy and data protection actually becomes even trickier once servicing has commenced. Thus, lawyers or professional external advisors often are not on board.
Certainly retaining external advice will cost some money, but we see it as a long-term investment in impeccable service, which is always on the safe side with regard to legal regulations.

I think this also contributed to EOS's excellent market standing today. Apart from the professional aspiration to do as good a job as we can, it is one of our core principles to make sure that we always comply with every single law.

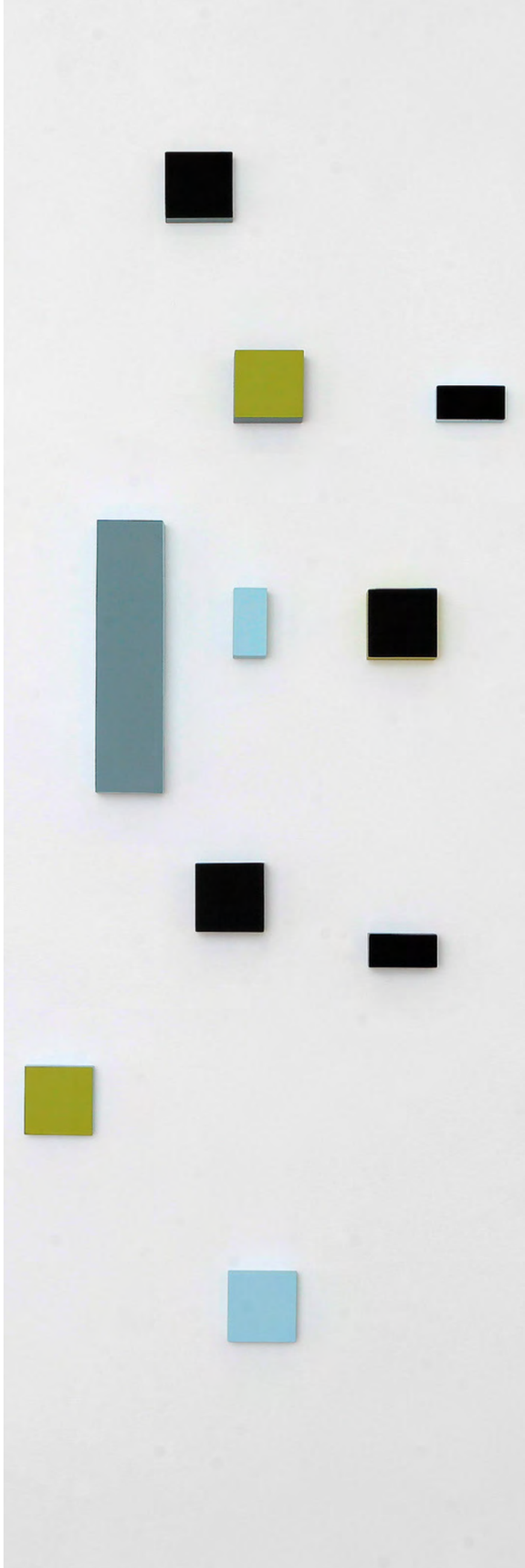
We do not see a difference whether a breach of banking secrecy or data protection would occur when implementing a portfolio transaction or during ongoing servicing. For this reason, we feel it is important to focus on this topic after a transaction has closed, and this includes continuing our cooperation with the right professionals.

How could we, the professional services industry, react to this? How could law firms assist?
Also, as one of our existing clients, what is on your wish list?
I would like to see transaction lawyers hand over and emphasise the relevant issues that were identified for a certain portfolio to the people involved in the actual servicing.

This normally should be easy, because the transaction lawyers are deeply involved anyway and have all the information, so a diligent handover, whether in the form of a compliance manual based on the due diligence findings or by means of compliance trainings, should be assured.

Usually this would not be included in a lawyer's scope of work for the transaction, but the industry as such should strive to raise more awareness of this issue so that people put it on their radars.

Thank you for the interview.



Current banking secrecy obligations in Austria

Stefan Paulmayer

The following gives an overview of current Austrian banking secrecy obligations and their impact on loan sale transactions.

It also proposes a new exemption from banking secrecy tailor-made for loan sale transactions – this would help reduce practical burdens for all parties involved.

> Credit institutions […] must not divulge or exploit secrets which are revealed or made accessible to them exclusively on the basis of business relations with customers […] (banking secrecy). […] The obligation to maintain secrecy applies for an indefinite period of time.
>
> § 38 (1) BWG

There is no **exemption** for loan sale / **portfolio sale transactions.**

THIS AGREEMENT
is dated 17 May 2017 and made between:

(A) [redacted], a limited liability company *(Gesellschaft mit beschränkter Haftung)* incorporated and existing under the laws of the Republic of Austria, having its registered office at [redacted] and being registered with the companies' register *(Firmenbuch)* of the regional court of [redacted] under registration number FN [redacted] as parent and borrower (the "**Parent**");

(B) [redacted], a limited liability company *(Gesellschaft mit beschränkter Haftung)* incorporated and existing under the laws of the Republic of Austria, having its registered office at [redacted] and being registered with the companies' register *(Firmenbuch)* of the regional [redacted] under registration number [redacted] as borrower (the "**Borrower**" or "[redacted]");

(C) [redacted], a limited liability company *(Gesellschaft mit beschränkter Haftung)* incorporated and existing under the laws of the Republic of Austria, having its registered office at [redacted] and being registered with the companies' register *(Firmenbuch)* of the regional court of [redacted] under registration number FN [redacted] as guarantor (the "Guarantor" or [redacted]); and

(D) **Bank AG,** a credit institution incorporated and existing under the laws of the Republic of Austria, having its registered office at Bankstraße 1, 1010 Wien and being registered with the companies' register *(Firmenbuch)* of the commercial court of Vienna *(Handelsgericht Wien)* under registration number 245265m, as original lender (the "**Original Lender**"), facility agent (the "**Agent**") and security agent (the "**Security Agent**")

PREAMBLE

1. WHEREAS, [redacted] and [redacted] (as defined below) are the ultimate legal and beneficial owners of the Parent and whereas the Parent has acquired all shares in [redacted] under and subject to the terms of the Acquisition Agreement (as defined below).

Currently, parties often implement work-arounds as a bypass – which, however, often only allow for limited disclosure of information to the purchaser of a loan portfolio:

- red / green data room structure with disclosure of sensitive information only to (financial and legal) advisors
- data trustee structure with disclosure to purchaser only in case of occurrence of certain trigger events (eg insolvency of seller etc)
- structuring the transaction as securitisation pursuant to CRR (requiring *inter alia* tranched refinancing and very limited business activities of purchaser)

Proposal for new exemption from banking secrecy for loan sale transactions:

"disclosure in connection with an (intended) full or partial transfer of exposure of the credit institution or the (full or partial) transfer of the risks thereunder to potential purchasers or assignees / transferees (as well as persons acting for such potential purchasers or assignees / transferees for the purposes of facilitating the relevant transaction), provided that such persons explicitly undertake in writing for the benefit of the customers of the credit institutions to keep the disclosed secrets confidential and not to pass them on to third parties."

Banking secrecy in CEE - one region, different rules.

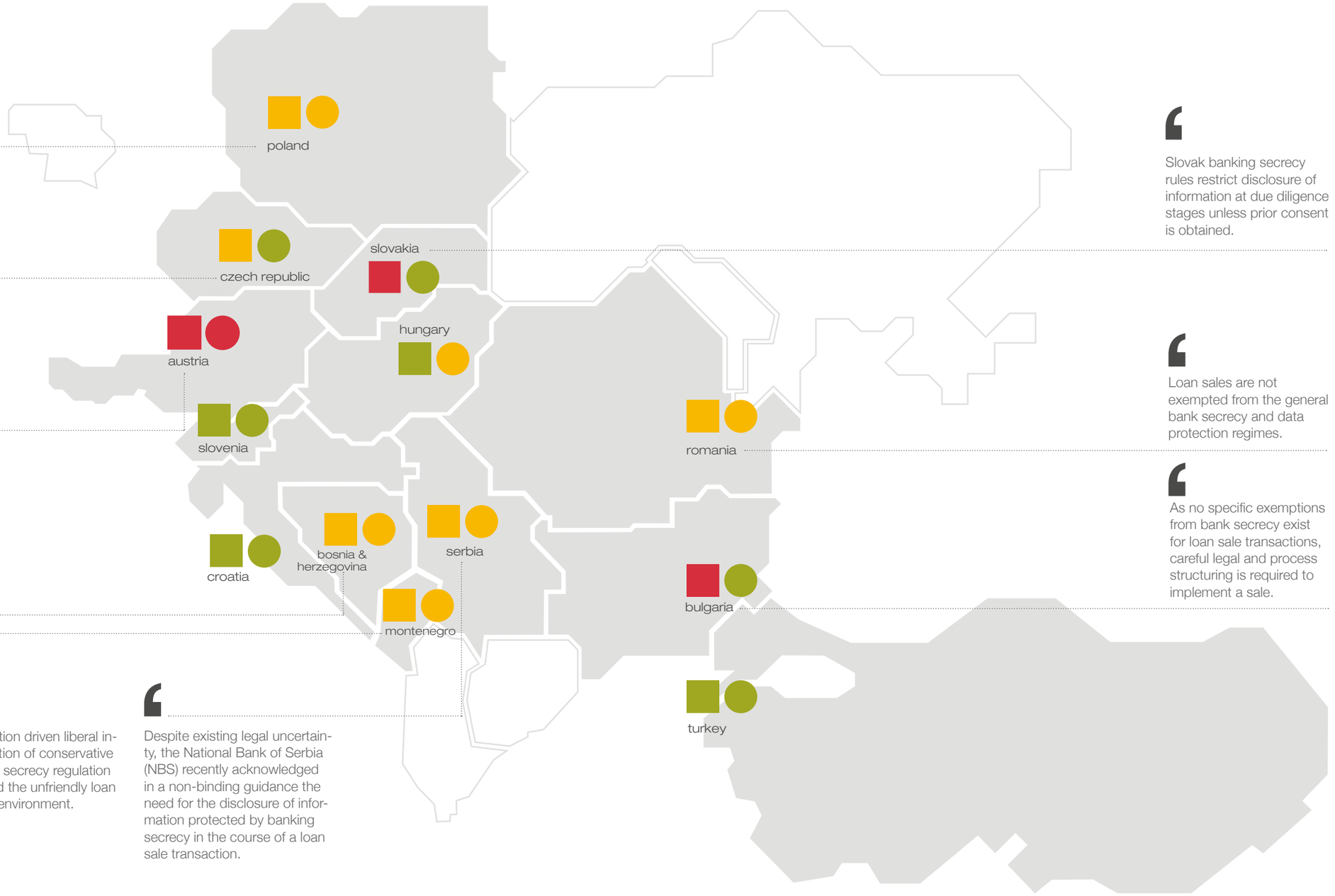
Despite ongoing harmonisation and the regulatory pressure on banks to reduce NPL quotas, banking secrecy rules in various jurisdictions still create hurdles to effectively implement loan sale transactions and hamper follow-on servicing. In the pages that follow, we provide a broad, simplified overview of how the rules per jurisdiction affect the legal environment in respect of these transactions and follow-on servicing.

Key

Loan transactions

Servicing

Red: Very stringent legal environment; very careful structuring required.
Yellow: Challenging legal environment, legal and regulatory restraints.
Green: Friendly legal environment and / or privileges for NPL trades / serving activities.



Banking secrecy exemptions exist; however only apply to the extent receivables are acquired by eligible entities.

Case law exists that supports the disclosure of protected information with respect to defaulting debtors.

Careful deal structuring and simple implementation of follow-on servicing is required as no applicable exemption from banking secrecy exists.

Under recently adopted banking legislation, information protected by banking secrecy may be disclosed in the context a of portfolio transaction.

Transaction driven liberal interpretation of conservative banking secrecy regulation softened the unfriendly loan trading environment.

Despite existing legal uncertainty, the National Bank of Serbia (NBS) recently acknowledged in a non-binding guidance the need for the disclosure of information protected by banking secrecy in the course of a loan sale transaction.

Slovak banking secrecy rules restrict disclosure of information at due diligence stages unless prior consent is obtained.

Loan sales are not exempted from the general bank secrecy and data protection regimes.

As no specific exemptions from bank secrecy exist for loan sale transactions, careful legal and process structuring is required to implement a sale.

Overview per jurisdiction continued

Laurenz Schwitzer
Austria

Whereas market participants have found practical solutions to address banking secrecy issues at the transaction level, there also needs to be a focus on remaining compliant during the servicing period of a portfolio.

As no specific exemptions from bank secrecy exist for loan sale transactions, careful legal and process structuring is required to implement a loan sale. Ultimately, there is legal uncertainty on whether transactions in breach of banking secrecy could be challenged / void.
We believe that market participants have found practical solutions to address banking secrecy issues at transaction stages, in particular via a staged disclosure of protected information and by application of the so-called "red room advisor" concept. However, there also needs to be a focus on remaining compliant during the servicing stages. In addition to proper knowledge transfer with respect to protected data, this also includes thorough compliance training of case handlers.

Vladimir Markuš
Bosnia & Herzegovina

Banks may disclose information protected by banking secrecy, provided that it is disclosed in the context of a portfolio transaction to the extent this would be within the "bank's interest" to achieve a sale.

The new banking legislation adopted in 2017 introduces detailed regulation on banking secrecy for the Federation of Bosnia and Herzegovina and Republika Srpska. The new law includes a clear definition of the scope of protected information and regulatory obligations to not disclose such information, and provides for statutory exceptions.
For instance, a bank is entitled to disclose protected information to the extent such a disclosure would be within the "bank's interest" during a loan sale. It is yet to be seen how the new law will be interpreted in practice.

Tsvetan Krumov | Milena Angelova
Bulgaria

Due to the lack of specific exemptions from banking secrecy for loan sale transactions, market participants are inclined not to disclose protected information prior to transaction signing.

As no specific exemptions from bank secrecy exist for loan sale transactions, careful legal and process structuring is required to implement a sale. For example, market participants may avoid breaches of banking secrecy by engaging legal / financial advisors to review protected information during negotiations, whereby a (potential) buyer would only receive data in an anonymised and aggregated form.
From the commercial side, we believe that overall market expectations for an increase in loan sales in Bulgaria did not materialise in 2017 mainly due to new accounting requirements for Bulgaria's banking sector, which are currently being implemented by the Bulgarian National Bank with effect as of 2018 (and in parallel to IFRS 9).

Ozren Kobsa
Croatia

The Croatian Credit Institution Act clearly provides for specific exemptions from banking secrecy with respect to loan sale transactions.

Pursuant to the law, banking secrecy shall not apply, *inter alia,* in cases when (i) the client explicitly agrees in writing that confidential information may be disclosed, (ii) that would enable a credit institution to realise its interest when selling client's receivables, or (iii) confidential information is exchanged within a group of credit institutions for risk management.
Whereas, the selling of NPL portfolios has been tested to be within a bank's justifiable interest, proper analysis as to whether this exemption also applies to performing portfolios is strongly advisable.

Natálie Rosová
Czech Republic

Case law exists that supports the disclosure of protected information with respect to defaulting debtors.

The Czech Supreme Court supports the view that bank secrecy requirements do not prevent a bank from assigning its receivables of defaulting debtors, provided that the assignment of such loans has not been contractually excluded.
Commercially, we expect less NPL activity due to dropping NPL ratios and overall improved NPL structures.

Gergely Szalóki
Hungary

The abolition of the eviction moratorium kick started NPL transactions and such measures were followed with further, mainly positive legislation.

The main hurdle remained unchanged though: the purchase of receivables is a licensed activity in Hungary. Apart from that, the Hungarian National Bank introduced certain guidelines aiming to protect the consumers' rights when loan agreements are terminated.
Nonetheless, the regulatory environment has generally improved in favour of banks, investors and servicers. One prominent example is the Hungarian National Bank's guideline addressing the issue of banking secrecy and concluding that banking secrets may be disclosed even for prospective buyers in a tender process (if such a buyer undertakes confidentiality).

Jovan Barović
Montenegro

Still absent regulators' recognition of arguably well founded liberal interpretation of strict banking secrecy rules, leaves loan trading susceptible to a certain degree to breach of banking secrecy risk.

Strict banking secrecy rules have been relaxed by established practice formed on a liberal interpretation based on the argument that debtors' interests cannot be harmed during a due diligence exercise if their identity remains undisclosed and that full disclosure can be made to a selected purchaser, as otherwise regulation explicitly regulating loan sales would be redundant. While practice based on this liberal interpretation inspires comfort, the susceptibility of loan trading to breach of banking secrecy risk is not ruled out by the regulator or courts.

Paweł Halwa | Weronika Kapica
Poland

Banking secrecy exemptions exist if portfolios are sold to securitisation funds or SPVs. A bank may also enter into sub-participation agreements with such entities.

Banking secrecy is exempted to the extent necessary to conclude and perform transfers of receivables to a securitisation fund. Such funds usually entrust servicing of acquired loans to a special servicing company (servicer), which requires authorisation of the Polish Financial Supervisory Authority. The secrecy exemption also applies to an agreement with a servicer. Both a fund and a servicer may collect and process personal data of a debtor only for purposes related to management of receivables. The banking secrecy exemption also extends to the sale of "lost receivables" and public sale of loans.

Costin Sandu
Romania

We expect that legal uncertainty regarding client data disclosure and increased regulatory constraints will increase the load of preparatory stages and will prompt a more cautious approach to portfolio transactions.

Portfolio transactions are not exempted from general bank secrecy and data protection regimes in Romania. Moreover, legitimate interest was not tested in court as grounds for disclosure of client data. New challenges are expected as well as a result of the increase of data protection requirements and update of the sanctioning regime, starting with the entry into force of the General Data Protection Regulation in May 2018. Nonetheless, we are confident that with sufficient and careful preparation these matters can be dealt with successfully.

Petar Kojdić
Serbia

Existing legal uncertainties have recently been addressed by guidance issued by the National Bank of Serbia that is friendly to loan trading. However, information protected by banking secrecy may also qualify as a business secret and could give rise to private enforcement of damages claims.

The National Bank of Serbia confirmed in its non-binding guidance to Serbian banks that a person to whom a bank assigns claims against its debtors is exempted from the banking secrecy regime, thereby addressing legal uncertainty about whether exemptions to banking secrecy as prescribed by the Banking Act may apply to secondary debt trading. However, a banking secret may still qualify as a business secret and aggravated assigned debtors might try to bring civil law damages claims against any person who has (allegedly) violated business secrets.

Soňa Hekelová
Slovakia

Slovak banking secrecy rules restrict the disclosure of information at due diligence stages unless the debtor is in default or prior consent is obtained.

Applicable banking secrecy rules do not provide any exemption for a disclosure at due diligence stages to (potential) buyers. Careful deal structuring or obtaining consent of debtors is therefore required.
As for the actual assignment itself (and follow-on servicing), the law provides for an exemption that a bank may assign its receivable against and provide the assignee with the necessary documentation without the debtors consent if the debtor, despite a written warning, is in default for more than 90 calendar days.

Vid Kobe
Slovenia

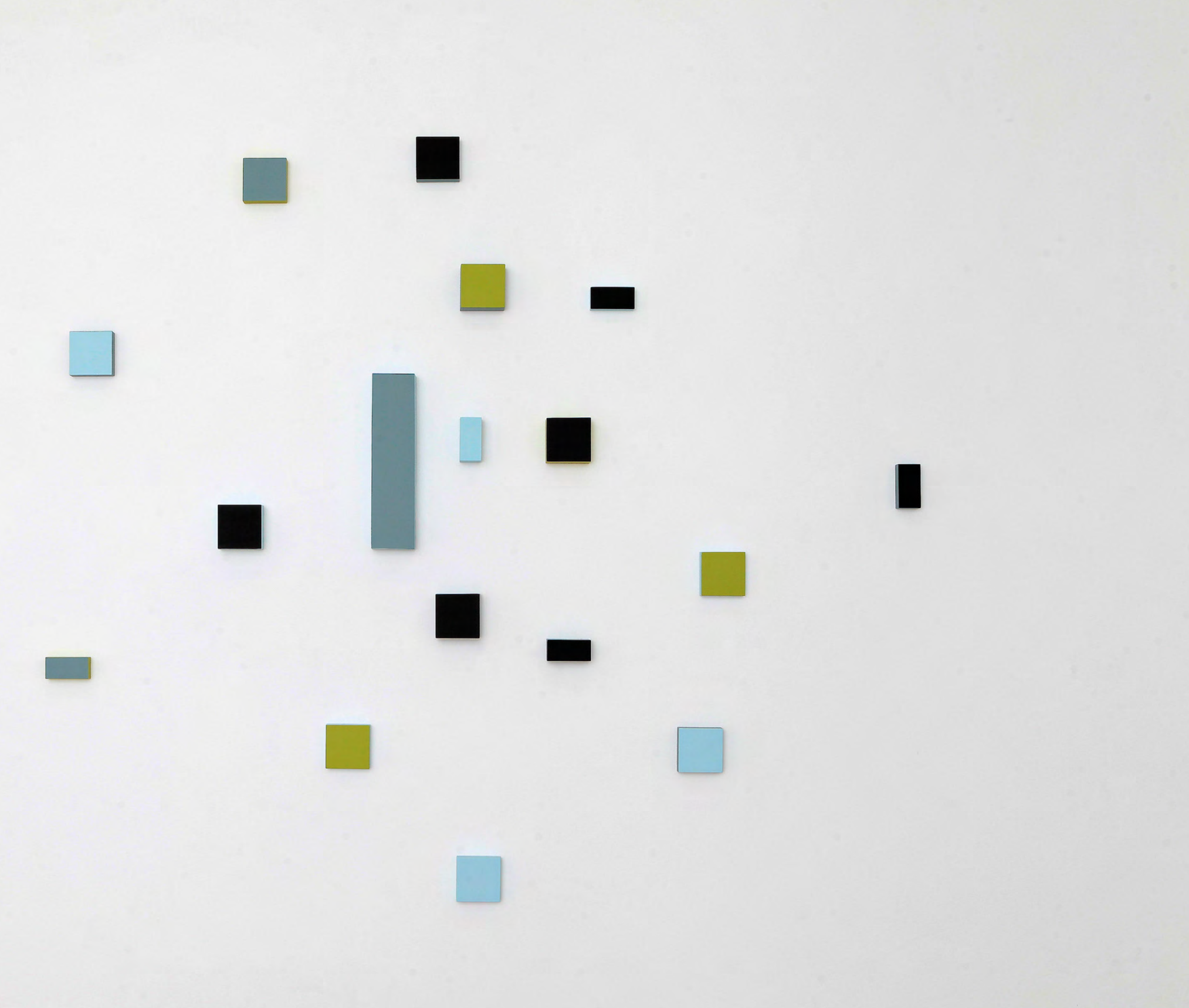
A pragmatic interpretation of the "proportionality test" imposed by Slovenian law provides for the required flexibility with respect to the disclosure of information.

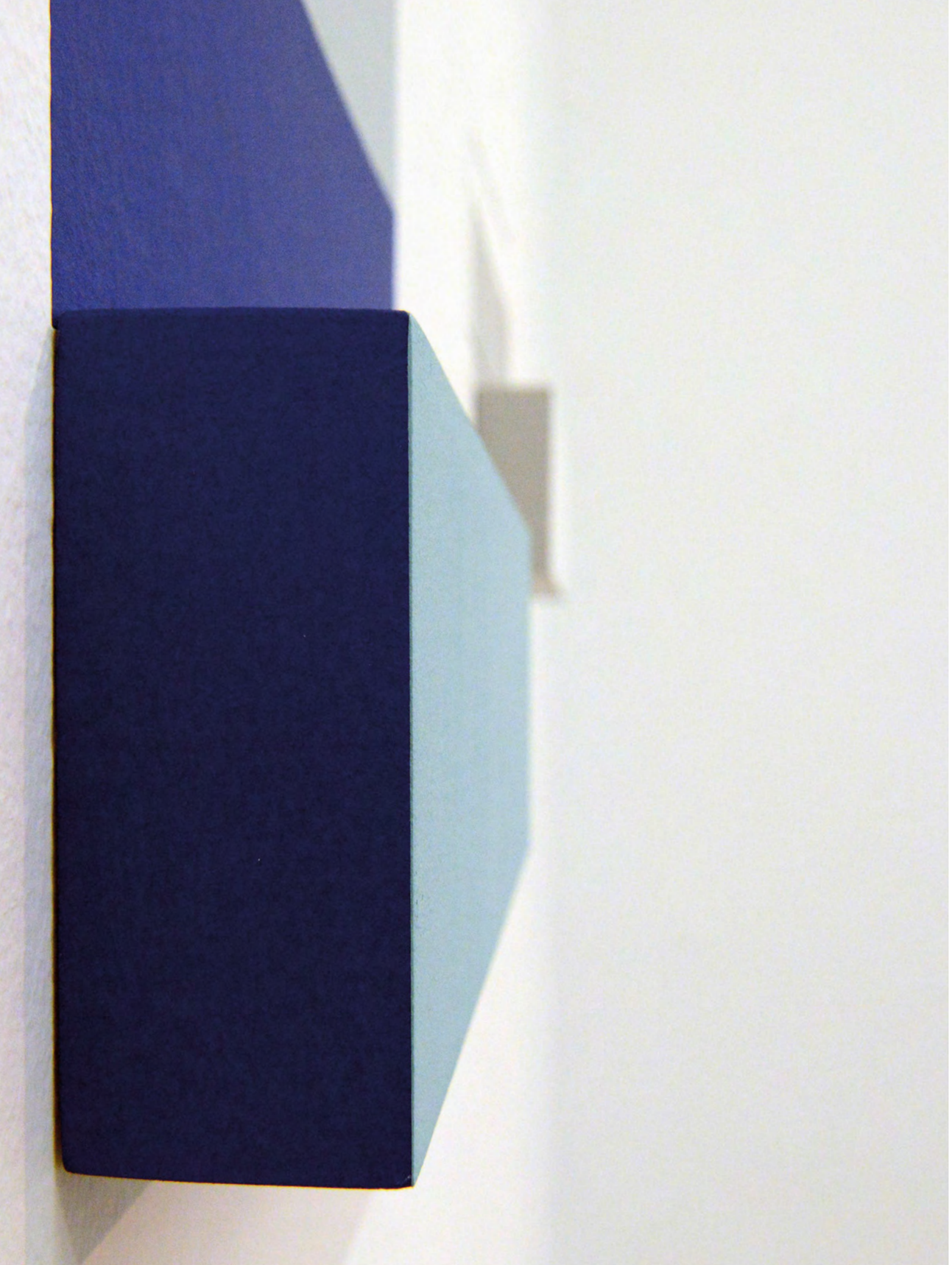
Slovenia has seen a lot of activity as regards portfolio deals in the past years and the players – in particular the local banking and legal community – have been quick to identify and adapt to the key legal challenges. Notably, the legal community was quick to embrace a pragmatic interpretation of the proportionality test imposed by the law in relation to permitted disclosure of information subject to banking secrecy. In a similar vein, transferability issues (in particular concerning certain types of security interests) were quickly overcome by means of alternative legal structures with commercially equivalent results, such as synthetic structures and corporate transactions.

Levent Çelepçi
Turkey

Exemptions to banking secrecy exist to allow for disclosure of protected information to specific regulated entities (set up to acquire loan portfolios), provided that a confidentiality agreement has been signed.

Turkish law provides sufficient exemptions from banking secrecy to allow for disclosure of protected information to specific regulated entities (ie asset management companies specifically licensed to take over NPLs), provided that a confidentiality agreement is entered into.
Turkish non-state-owned banks have been quite active in terms of transferring their NPL portfolios to such entities. In 2017, Turkish state-owned banks have also been given the green light (from a banking secrecy perspective) to transfer their NPL portfolios.





02 compliance & white collar crime

Criminal Procedural Law vs Individual Privacy / Liberty

Criminal procedural law vs individual privacy / liberty

Klara Kiehl | Michael Lindtner | Matthias Cernusca

Privacy is a very delicate issue from the perspective of criminal (procedural) law. For their investigative activities, state authorities are granted various rights which interfere with the privacy of the individual.

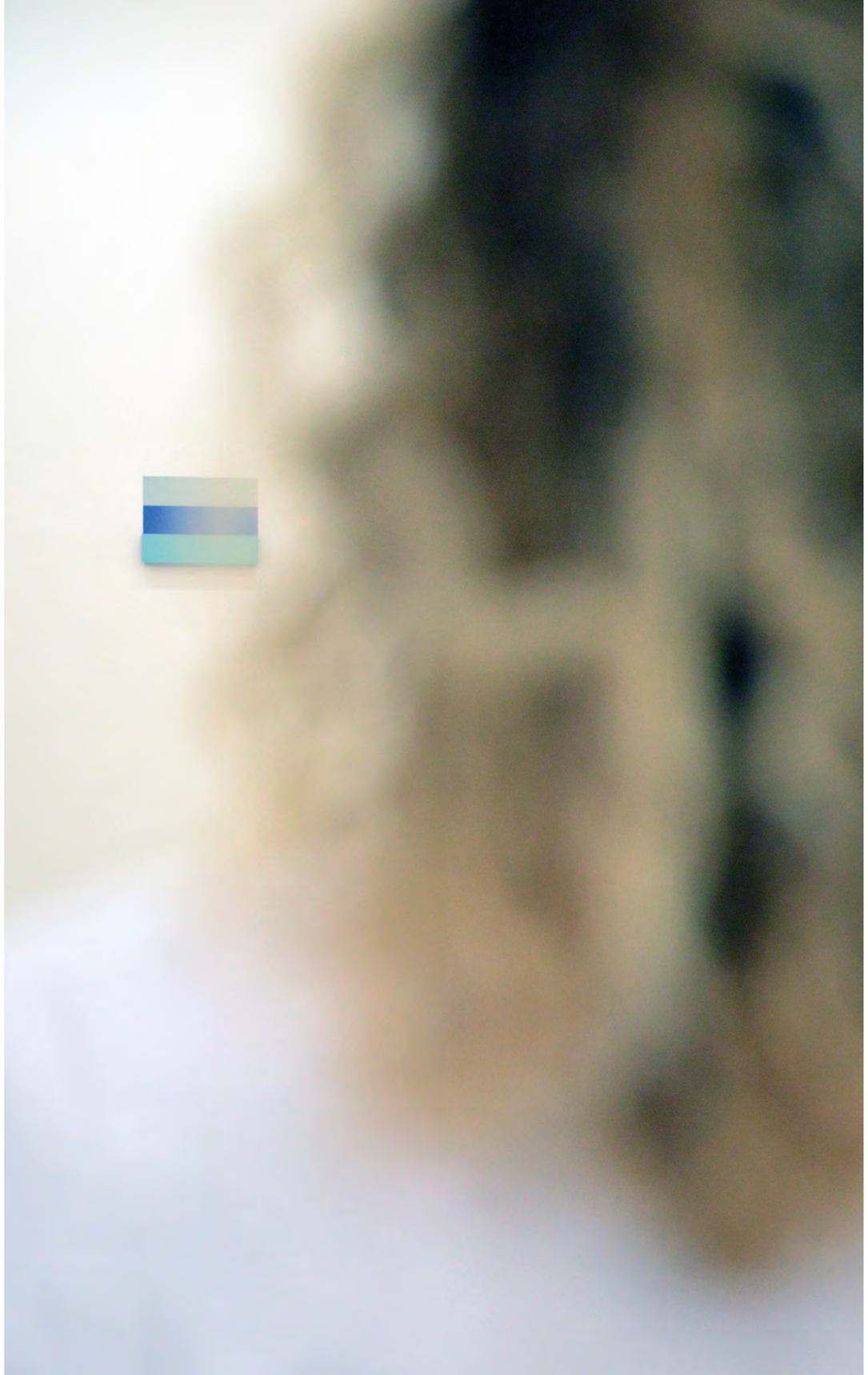
A prominent example is the possibility for state authorities to conduct house searches. Such house searches might take place not only at private homes, but also in the office buildings or factory sites of enterprises. When an enterprise is the target of the house search, it is the privacy of the enterprise which is at stake. In all instances, it is of utmost importance to minimise the detrimental effect of a house search. We have compiled a list of important do's and don'ts.

Another intricate issue from the perspective of criminal law and privacy is the recording of conversations. Many questions are still unresolved from a legal perspective. See more on that in our fictional interview...

Prosecution authorities have become more active over the past few years. House searches are no longer fantasy, but a stark reality. So what to do when the prosecutor comes knocking on your door? Some of the most important measures are outlined below from an Austrian law perspective. Some issues may have to be handled differently depending on your jurisdiction, so always consult your lawyer!

- Require the officers to show their IDs.
- Ask to see the search warrant.
- What does the search warrant cover?
- Who is the defendant?
- Call your lawyer.
- Ask the authorities to wait with the house search until your lawyer arrives.
- Do not to grant a "voluntary insight" to the authorities.
- Do not delete any electronic data nor destroy any paper documents.
- Do not let the authorities search the premises alone.
- Cooperate to the extent necessary and create an atmosphere of trust – but be aware of and insist on your rights.
- Prevent the authorities from seizing documents / data outside the scope of the search warrant. If they nevertheless insist, raise an explicit veto to the authorities!
- Prevent the authorities from seizing documents / data protected by attorney client privilege. If they nevertheless insist, raise an explicit veto to the authorities!
- The basic rule is that authorities should only take copies with them.
- Make a second copy of seized documents / data for your internal documentation.
- Watch out for and avoid subtle interrogation by officers!
- Insist on formal interrogation and insist on your rights, which are different depending on whether you are interrogated as a witness or defendant. Ask to have your lawyer present at the interrogation!
- Handle the PR issue carefully – avoid internal leaks.

Plan what to do beforehand, so that if the prosecutor indeed comes knocking you will be prepared!



What I always wanted to ask a lawyer… "recording" (Austrian law perspective)

Bamboozled again! The good old handshake agreements of the old days apparently died. Next time I'll wear a wire and record everything to bust these people. But is this legal? Maybe I should ask my lawyer first…

First you need to distinguish between the questions "Is recording conversations as such illegal?" and "Are you permitted to subsequently use such recordings?"

In a nutshell, these issues generally require a balancing of interests, namely those of the recorded person and the recording person. It is a very delicate discussion, since the private sphere of the persons involved is highly affected. In some cases the recording of conversations is prohibited explicitly by law. Nonetheless, many legal questions are still unresolved in this field.

So, do I risk criminal prosecution if I record conversations?
This depends on the situation. If you were a participant in the conversation, secretly recording it is not a crime. But recording the private conversations of third parties is a crime.

In both cases, the subsequent disclosure or circulation of the audio recording without the consent of the recorded person is also a crime.

OK, so as long as I'm a party to the conversation, I am permitted to record it, right?
From the criminal law perspective, yes. However, don't forget the civil law perspective! There is a high risk that the recorded person will have civil law claims, like damage claims or removal claims, if he / she did not agree with the recording.

So can I use recordings at least subsequently as evidence in proceedings?
There is no general rule in Austrian procedural law prohibiting the use of recordings as evidence, but that does not mean that any recording can be used as evidence without limitation. The admissibility requirements and the actual legal boundaries of submitting recordings as evidence are still unclear in many respects.

Nonetheless, courts generally tend to rule that recordings can be used as evidence for defence against unjustified claims. Therefore, there are cases where the recording of conversations has advantages covered by law. But this must be assessed carefully beforehand.

Austrian criminal law provides clear rules regarding the legality of recording of conversations. From the civil and procedural law perspective, however, the issue is murkier.

Ask your lawyer beforehand!

03 corporate / m&a
Disclosure

Disclosure in the context of private m&a transactions

Thomas Kulnigg

In which context is "disclosure" relevant in private m&a transactions?

Disclosure is a key element of private m&a transactions. It is primarily used in the context of representations and warranties as well as for procedural / structural aspects.

How is disclosure relevant for representations and warranties for a buyer?
The buyer makes an investment decision based on its knowledge of the target business, which is derived mainly from information about the target business disclosed by the seller (disclosed information). A prudent buyer will want to assure the assumptions underlying its investment decision (investment assumptions) via representations and warranties. Disclosed information is therefore used to determine the scope of the representations and warranties (eg if a target business utilises a key supplier, the buyer will want protection via representations and warranties that the supply agreement with that key supplier is valid and has not been terminated).

How is disclosure relevant for representations and warranties for a seller?
For the seller, the disclosed information ideally forms the basis for its disclosure defence.

What is a "disclosure defence"?
The disclosure defence allows a seller to disclaim liability for breaches of representations and warranties if the underlying matters have been disclosed to the buyer. This is typically as heavily negotiated as the scope of the representations and warranties themselves, as the parties' interests are contrary. A buyer will want a catalogue of representations and warranties that is not qualified by disclosed information, whereas the seller will want all information available on the target business to qualify its liability.

How do parties typically resolve the "disclosure defence" discussion?
Typically, the parties either agree that only specific matters disclosed in a transaction document (or even in a separate disclosure letter) are deemed "disclosed" and thereby limit the seller's liability (the buyer-friendly approach) or the parties agree that the information

disclosed during the due diligence will limit the seller's liability (the seller-friendly approach, typically seen in private m&a transactions). In the latter case, parties can further tweak the "disclosure standard", ie which level the disclosure must reach to limit the seller's liability. Here is a typical definition that further determines the disclosure standard:

"Disclosed" means any disclosure in the Data Room that is sufficiently detailed to identify the nature and scope of the matter disclosed and to enable a reasonably experienced purchaser active in the Target Group's sector, advised by professional advisors, to assess its impact on the relevant Target Company and the Target Companies taken as a whole.

How is the disclosure defence applied in practice?
In practice, a disclosure defence is complex, as whether a matter can be identified as a breach of warranty is always subjective. Sellers should therefore ensure that known issues are properly disclosed in a way that any investor can identify the issue.

What is a "disclosure warranty" and is it market standard?
It is said that disclosure warranties have their origin in Rule 10b5 of the US Securities and Exchange Act of 1934, which determines the liability of the company and the underwriters if a prospectus contains any untrue statement of a material fact or omits material facts necessary to ensure that the statements made in the prospectus are not misleading. To mitigate risks, underwriters typically request so called "10b-5 disclosure letters" from both their and the company's counsels to ensure the absence of any such misstatement or omission. Investors in private m&a transactions took that concept and translated it into the private m&a world by requesting the seller to warrant that the information disclosed is true, accurate, complete and not misleading. Here is a typical buyer-friendly disclosure warranty:

1.1 All information contained in or referred to in the Data Room or which has otherwise been disclosed to the Purchaser or its advisors is true and accurate in all respects.

1.2 The Seller has disclosed all information relating to the Target Group and their respective businesses, assets and undertakings (including financial information) which may be relevant to a purchaser's decision to enter into this Agreement and there is no fact, matter or circumstance which renders any such information misleading because of any omission, ambiguity or for any other reason.

From a seller's perspective, such a warranty is difficult as the question whether the disclosed information is "complete" and "not misleading" is very subjective and there are no rules that define these terms. A prudent seller will therefore try to limit such warranties as much as possible.

How is disclosure relevant for procedural / structural aspects?
Disclosed information further helps to migrate the target business into the buyer group, including defining requirements for transitional services. A prudent buyer will thus review as part of its due diligence if and to what extent the target business can operate on its own or whether it is dependent on services from the seller's group. Also, change of control clauses and other matters that are relevant for structuring a transaction can be derived from the disclosed information.

> In practice, a disclosure defence is complex, as whether a matter can be identified as a breach of warranty is always subjective. Sellers should therefore ensure that known issues are properly disclosed in a way that any investor can identify the issue.

Supervisory Board: Disclosure of conflicts of interest and confidential information

Maximilian Lang

> A potential conflict of interest does not prevent a person's election to the supervisory board of an Austrian joint stock corporation or societas europaea. It is generally accepted that supervisory board members may have interests that differ from those of the company.

Prior to their election to the supervisory board of an Austrian stock corporation or, in case of a two-tier governance system, societas europaea candidates have to disclose to the shareholders their qualifications, profession and other functions as well as all circumstances that may create the appearance of a conflict of interest.

Usually this is done by submitting a CV and a statement on (no) conflicts of interest with the company, which then discloses this information to the shareholders, or, in the case of a listed company, publishes the information on its website. However, a potential conflict of interest does not prevent a person's election to the supervisory board, as being a supervisory board member of an Austrian joint stock corporation or societas europaea is a part time job. Therefore, it is generally accepted that supervisory board members may have interests that differ from those of the company. Besides certain incompatibility rules and statutory restrictions on the exercise of voting rights in shareholders' meetings, such conflicts are not generally prohibited, but have to be disclosed by the supervisory board member and dealt with on a case-by-case basis. Therefore, supervisory board members are under a constant obligation to disclose potential conflicts of interest to the supervisory board and, in case of a conflict of interest, to abstain from voting on the specific matter. In case of non-compliance with this obligation, the chairman of the supervisory board must not count that member's vote. In exceptional cases, conflicted supervisory board members may be excluded from supervisory board meetings by majority vote.

Disclosure of confidential information to individual (controlling) shareholders
Control of the supervisory board is the key to control over an Austrian stock corporation. Although legally independent, individual supervisory board members are therefore often elected and see themselves as representing the interests of significant / controlling shareholders. In practice, this means sharing and discussing confidential information (such as trade secrets and information relating to the company's business operations) with significant / controlling shareholders. This conflicts with statutory law requiring supervisory board members to keep confidential and not to disclose confidential company information to third parties. Non-compliance with

confidentiality obligations may result in damage claims by the company against the respective supervisory board member, constitutes important cause for early recall by the competent court upon request of a 10% minority and, in exceptional cases, may even result in criminal penalties (eg under the Unfair Competition Act).

However, it is generally accepted that in a group of companies (Konzern), supervisory board members of the subsidiary company may disclose confidential information to the parent company.

Moreover, legal and commercial practice accepts that supervisory board members not elected by the shareholders' meeting, but delegated based on special delegation rights set forth in the company's articles of association or vested in the holder of a "golden" registered share may, as an exception to the general duty of confidentiality applicable to supervisory board members, disclose confidential information to the delegating shareholder. The same applies to supervisory board members elected based on a syndicate agreement between controlling shareholders. The delegating shareholder and the delegated supervisory board member may also enter into a formal mandate agreement pursuant to which the supervisory board member agrees to keep the shareholder informed on confidential matters concerning the company and, subject to restrictions, to discuss and agree on the voting in the supervisory board. Nevertheless, this exemption from the general duty of confidentiality is not absolute. In no case may the company be harmed by the disclosure (eg disclosure of information for competition purposes is not permitted). In case of a listed company, further rules may apply with regard to the disclosure of inside information or the obligation to disclose transactions with securities in the company (director's dealing).

Although legally independent, individual supervisory board members are in practice often elected as representatives of the interests of significant / controlling shareholders.

Delegated supervisory board members and delegating shareholders may enter into mandate agreements regarding the disclosure of confidential information and the exercise of voting rights.

Privacy-related representations in m&a agreements

Clemens Rainer | Paul Nimmerfall

Companies regularly store information about their customers, clients, employees, investors, partners and vendors. Privacy and data security are therefore important aspects of most m&a transactions. Although the risk of non-compliance with privacy laws may result in severe negative consequences, many m&a agreements still lack adequate privacy-related representations and warranties (R&W). This article discusses the rising importance of privacy issues and how to approach them effectively.

Know who you are and what you acquire

In order to frame an appropriate set of R&W, it is of vital importance for both parties to not only understand the target's business in general but also the privacy-related environment in which the target conducts its business (eg nature and amount of collected personal information, storage location and applicable privacy-related legal provisions).

By properly assessing privacy and data security issues in the course of a due diligence, a buyer can manage transactional risks and ensure that m&a agreements contain provisions that adequately address the target's privacy-related issues. A thoroughly conducted privacy-related due diligence should therefore cover the following:

- the existence of adequate policies and procedures (eg data security governance, external or internal audits);
- past breaches and security incidents (eg history of breaches, pending and threatened litigations);
- future legal requirements (eg General
- Data Protection Regulation – GDPR);
- social media material (social media presence, activities and policies);
- employment privacy (eg e-mail use regulations and other aspects of employment privacy);
- international considerations (applicability of international privacy-related laws).

Default clause might not be enough

In many cases, practitioners simply rely on standard "compliance-with-laws-representations"; but these often do not adequately address privacy issues and usually do not provide enough protection for buyers.

Of course, privacy-related representations should cover compliance with privacy laws – but they should not stop there. A sophisticated set of R&W should in particular cover the following:

Compliance

- with all laws, including applicable laws related to privacy, data security and the processing of personal information, including (but not limited to) the requirement to (i) gain data subjects' con sent to transfer and use of their data and (ii) file any registrations with the applicable data protection authority;
- with the target's own policies, representations to consumers & employees, contracts and applicable industry standards;
- with future legal requirements (eg ap propriate procedures to ensure compliance with the GDPR);
- with notices, consents and other information provided to data subjects regarding the processing of personal information;

Implementation

- of adequate policies and procedures to ensure continued compliance with all applicable data protection and privacy provisions;
- of data security measures, including measures which are not necessarily required by law;

Data security

- no loss, damage or unauthorised access, use, modification or other misuse of any personally identifiable information maintained by or on behalf of the target;
- no claim or action with respect to loss, damage or unauthorised access, use, modification or other misuse of any such information; no reasonable basis for any such claim or action;

Disputes

- no past, pending or threatened privacy-related disputes, claims or complaints with / by an individual or an administrative authority.

Caution is needed

This article aims to build awareness. Sophisticated privacy-related R&W in m&a agreements can indeed offer a certain level of comfort to buyers, but they are not a universal cure. Even if damages are awarded as a result of accurately drafted R&W, they may not be sufficient to compensate for the type of public relations and customer relationship damage often associated with privacy failures.

Disclosure obligations under the Austrian Stock Exchange Act

Sascha Schulz

> In a nutshell, the rules inhibit secret stake building or exercising control by the bidder without prior disclosure.

Due to their volume and value, transactions in listed companies regularly affect a variety of different stakeholders, from minority shareholders through to creditors, employees and the public interest.

Whereas a control-seeking bidder is interested in acquiring a prospective target quietly for an attractive price and with the ability to implement control as soon as possible, minority shareholders, in particular activists, will be interested in being informed about any changes in the target company's control situation as soon as possible, as they are heavily dependent on the new core shareholder's corporate decisions and will exit at the most favourable price possible. Creditors, meanwhile, will be interested in a steady loan-to-value ratio, and employees will demand job security. Taking these and other conflicting interests into account, the Austrian legal framework provides for a number of disclosure rules to the detriment of the bidder and limiting its privacy.

One of the bidder's key disclosure obligations is set in the Austrian Stock Exchange Act. Originating from the European Transparency Directive (last amended by 2013/50/EU), a bidder that reaches, crosses or falls below certain thresholds in a target company's voting rights starting with 4%, 5% to 50% in increments of 5%, 75% and ending at a level of 90% is obliged to notify the target company, the Vienna Stock Exchange and the Financial Market Authority within two trading days. Subsequently, the target company has to inform the market by a public announcement. Failing to provide the necessary information to the above entities will be sanctioned by suspension of the bidder's voting rights and fines that could reach up to EUR 10 million or 5% of the bidder's total annual net revenues.

In order to prevent evasion, shares with voting rights that are *inter alia* held by a bidder's subsidiary or other persons acting in concert with the bidder shall be attributed to the bidder, too. Finally, the notification obligation includes financial instruments in case a threshold pursuant to the Stock Exchange Act is reached or crossed. Financial instruments can either be arrangements that give the bidder a right to acquire (or the discretion as to its right to acquire) target company shares with voting rights or other instruments, which may not provide an acquisition right, but which are referenced to target company shares and provide a similar economic effect, whether or not they confer a right to a physical settlement. Most importantly, for the purpose of calculating the overall number of the bidder's voting rights in a target company, (in) direct shareholdings and financial instruments shall be aggregated.

In a nutshell, the rules inhibit secret stake building or exercising control by the bidder without prior disclosure. Other stakeholders are able to react appropriately to changes in the shareholder structure at an early stage. On the other hand, bidders who intend to acquire a significant stake or control need to carefully prepare their acquisition plan and move forward quickly, as privacy in listed companies is sacrificed for the benefit of transparency.

Mandatory registration of beneficial owners introduced for all Czech entities

Vladimír Čížek | Jitka Kadlčíková

As of 1 January 2018, all legal entities registered in the Czech commercial register must submit and register information about their beneficial owner(s) in the beneficial ownership register.

What does the beneficial owner registration requirement comprise?
Generally, the requirement includes the obligation to disclose and register information about beneficial owner(s), including their name, date of birth, place of residence and citizenship, and most importantly, details about the beneficial owner's voting rights or shares in the legal entity, or other facts establishing that he or she is a beneficial owner of the legal entity.

Who is affected by this obligation?
Practically, all legal entities that are registered in Czech public registers, ie in the Register of Associations (spolkový rejstřík), Register of Foundations (nadační rejstřík), Register of Institutes (rejstřík ústavů), Register of Associations of Unit Owners (rejstřík společenství vlastníků jednotek), Commercial Register (obchodní rejstřík) and Register of Public Service Companies (rejstřík obecně prospěšných společností), as well as all trusts registered in the List of Trusts (evidence svěřenských fondů), will need to disclose and register information about their beneficial owner(s) in the Beneficial Ownership Register by certain deadlines.

How do we assess who a beneficial owner is?
A beneficial owner is any natural person who has – by factual or legal means – directly or indirectly a material influence over a legal entity, trust or other entity without legal personality, provided that such influence is exercised. In principal, a natural person who owns 25 % of the shares in a legal entity or is entitled to equivalent voting rights or is a beneficiary of an equivalent stake in profits of such an entity is considered to be a beneficial owner. Most importantly, should the management of a legal entity still be unable to positively confirm the identity of such a person after a due and careful examination, then the statutory body of that legal entity will be considered the beneficial owner(s).

Who is obliged to discharge the registration duty?
Generally, members of statutory bodies of the respective legal entities are obliged to file a submission for registration of the information of the beneficial owner in the register.

Are there any associated costs?
Yes, the registration is subject to a court fee of CZK 1,000 (ie approx EUR 38.50). In each case, there is a one-year fee waiver for legal entities registered in public registers before 1 January 2018.

What are the consequences of non-compliance?
Should the relevant legal entity fail to register the information of the beneficial owner, it may be subject to a penalty of up to CZK 100,000 (ie approx EUR 3,850). There is a risk that such a penalty may be imposed recurrently should the failure remain unremedied. In addition, the members of the entity's statutory bodies may be held liable for breach of their duty to act with due managerial care in this respect.

What needs to be done and by when?
Currently, all affected legal entities have to wait for the Ministry of Justice of the Czech Republic to publish (with a final date not yet set) implementing legislation providing details of beneficial owner(s) registration forms. In the meantime, we encourage the affected legal entities to collect all documentary evidence and information concerning identification of their beneficial owner(s) and to proceed to verify their status. Once the registration forms become available, the members of the legal entity's statutory body need to file the submission for registration of the beneficial owner(s) accompanied by the respective information evidencing this. The Commercial Court normally registers the information within five business days from lodgement of the submission. Legal entities registered in public registers before 1 January 2018 should, as we understand the rationale of the legislation (with the law being unclear on timing), submit so that the information on beneficial owners is registered as of 31 December 2018 at the latest. For other legal entities, we believe that the deadline for submission will expire on 1 January 2020 (or one year earlier, depending on the interpretation of the ambiguous legislation).

Purpose: to prevent corruption, money laundering and terrorism financing via increased transparency of ownership of defined legal entities.
Affected / obliged legal entities: all legal entities registered in Czech public registers.
New managerial duties: management is obliged to fulfil the registration obligation on behalf of the relevant legal entity and, in certain cases, may be considered beneficial owner(s).
Sanctions: a penalty for non-compliance may be imposed upon the affected legal entity.
Deadlines: legal entities registered in the Commercial Register must likely discharge the registration obligation by 31 December 2018; for other legal entities the deadline for submission expires likely on 1 January 2020.

Compulsory disclosure of beneficial owners when doing business with a state in Slovakia


Soňa Hekelová | Michal Lučivjanský

> The Anti-Letterbox Act is strict, with broad application to many legal entities in Slovakia and an almost draconian system of sanctions.

From early 2017, legal entities doing business with a state or holding specific licences have had to register information about their beneficial owner(s) in a publicly available registry.

A specific regime for the disclosure of beneficial owners (independent from the regime under the new Fourth Money Laundering Directive) was introduced in Slovakia at the beginning of the year by the so-called Anti-Letterbox Act, whose main purpose is to combat "shell" or "letterbox" companies that receive public funds and do business with public authorities. In practice, however, it affects almost all private entities doing business with the Slovak state and authorities.

Registry and affected entities

Under the Anti-Letterbox Act, certain entities are required to register in the registry of partners of the public sector (the "Registry"), mainly those providing services or goods through public procurement or concluding other agreements with state authorities. Nevertheless, the obligation also applies to health care providers and entities supplying them, entities applying for investment aid from the Slovak state (or EU funds), and holders of licences in certain regulated industries, such as energy or mining.

The ultimate beneficial owner is a natural person actually controlling the respective company, in particular a natural person who directly or indirectly holds at least 25% of shares or voting rights in the legal entity or has other controlling rights over it. There are specific rules for publicly traded companies. As the Registry is accessible online to everyone free of charge, in practice everyone is able to see identification data on the beneficial owners, who are subject to public scrutiny (especially in cases when a company takes part in a business case / public procurement that is being covered by the media).

Legal entities cannot file the application for registration, only an authorised person, who under the Anti-Letterbox Act must be one of the following: (i) attorney at law; (ii) notary; (iii) bank; (iv) auditor; or (v) tax advisor, in each case with registered seat in Slovakia. Before submitting the application, the authorised person must duly verify the information on the ultimate beneficial owners and must conduct an independent review of the company's ownership structure.

Sanctions

The Anti-Letterbox Act introduces strict sanctions for non-compliance with the registration obligation. For instance, if inaccurate information is provided to the Registry, the following sanctions may apply:

- a fine on the registered legal entity corresponding to the amount of economic benefits received from the public sector or up to EUR 1 million if the amount cannot be determined;
- a fine of EUR 10,000 – 100,000 for each of the managing directors of the registered entity, who are strictly liable regardless of culpability and without possibility of release; or
- loss of licence in specific cases (eg energy licence).

Applicability in practice

The Anti-Letterbox Act is strict, with broad application to many legal entities in Slovakia and an almost draconian system of sanctions. It also causes problems for foreign private owners of Slovak entities who want to retain their privacy. At this point, whether it will achieve its main aim is doubtful.

Romanian m&a on trial: Translation of international standards into local m&a transactions

Mădălina Neagu

Romanian private m&a has constantly sought to align itself to the international standards of transaction documentation, with some distinctions in terms of scope and interpretations of traditional m&a concepts still to be considered.

Ever since the late 1990s, when large international players arrived in Romania and began acquiring strategic assets, the private m&a market has been quick to adapt to the standards of international transactions. Nowadays, Romanian m&a transactions are almost universally founded on Anglo-Saxon-inspired documentation, juggling a wide range of concepts such as disclosures, material adverse change, representations, warranties and specific indemnities, some of which still lack proper translation into Romanian law.

While in the case of large deals (in excess of EUR 100 million) you can still find transactions governed by foreign law (usually UK law), most private m&a transactions are governed by domestic law. Little wonder, then, that the foreign parties to these transactions often ask whether Romanian law is different from that of more traditional m&a jurisdictions.

m&a transactions in Romania are essentially governed by the general principles of sale and purchase laid down in the Civil Code, which, like in other countries, provides for freedom of contract, the duty to negotiate in good faith, and penalties for fraudulent negotiation of contractual terms.

While the format of Romanian transactions is similar to that of share purchase agreements under English law, not all English law concepts have the same meaning when used in local deals. Common law systems are constantly evolving and being reshaped by case law and new interpretations. Compared to the common law system, the Romanian legal system may appear more rigid and codified, but lacking the benefit of precedents. Furthermore, even where such precedents exist, they are sometimes inconsistent, and in any case, they are not formally binding to other courts called to rule on similar cases.

A good example of this is the concept of full and fair disclosure. With the aid of jurisprudence, English law has polished the concept of "full and fair", giving its users plenty of guidelines as to how detailed the disclosure level should be for a reasonable buyer to properly understand the disclosure and its implications for the warranty in question. This further evolved towards concepts such as "disclosure letter" or "disclosure bundle" and "specific disclosure", which are practically market standard for transactions governed by English law.

At the opposite end, an SPA under Romanian law would certainly not prohibit a contractually built concept of "full and fair disclosure", but the legal system would likely lack the examples required to add the proper content to this requirement and determine the practical implications and limitations thereto. This deficiency would need to be compensated by more elaborate drafting, setting out not only the content of disclosures (information provided through the data room, public registries, transaction process), but also the quality standard of the information disclosed. A topic closely connected with disclosure is that of representations and warranties. Under a common law system, representation and warranties arose as a reaction of the purchasers seeking to redress the consequences of the caveat emptor (buyer beware) principle (the seller having no legal obligation to provide warranties).

From this perspective, Romanian law positions itself as more purchaser-friendly, already providing reasonable legal protection though the warranties on title and use (raspunderea pentru evictiune) and defects (raspundere pentru vicii), and allowing the purchaser to claim a reduction of the purchase price or, depending on the gravity of the breach, the termination of the agreement. International standard warranties have nevertheless been adopted into local m&a and are almost universal in private deals, although without the legal distinction between warranties and representations, but rather under the general concept of warranties.

Where Romanian law comes closer to the equivalent Anglo-Saxon concept is on the legal sanction applicable to sellers' fraudulent actions. Romanian law penalises fraudulent misrepresentation, providing that all contractual limitations of a seller's liability cease to apply if the seller's breach is attributable to intention or gross negligence. The Romanian standard appears to be even broader, since UK law refers to intentional acts (fraud and fraudulent misrepresentation), while Romanian law applies the same sanction to both intention and gross negligence. The legal consequence is similar, ie liability cannot be contractually excluded or limited in case of a breach of contractual duties attributable to intention or gross negligence.

Non-financial reporting in Slovenia

Marko Prušnik | Matej Vošner

> The newly adopted additional reporting requirements will likely lead to changes in the mindset of entrepreneurs in relation to certain aspects that are still partially under developed in some companies and business sectors in Slovenia, such as sustainability of business operations, compliance and diversity / HR.

A recent amendment to the Slovenian Commercial Companies Act obliges public-interest companies to provide corporate governance and other non-financial statements in their annual reports.

Background and overview
In 2017, the National Assembly of the Republic of Slovenia adopted another amendment to the Slovenian Commercial Companies Act (Zakon o gospodarskih družbah, ZGD1J), which harmonises certain aspects of Slovenian corporate law with Directives 2014/95/EU and 2005/56/EC of the European Parliament and of the Council, and introduces some other changes in the national legislation.

The biggest change to the Slovenian corporate law landscape will be brought about by the mandatory inclusion of certain non-financial (corporate governance and other) statements in the annual reports of public-interest companies.

Non-financial reporting
Based on this latest amendment of the Commercial Companies Act, large Slovenian public-interest companies (ie listed companies, insurance companies and credit institutions) with more than 500 employees will be obliged to include detailed statements on environmental, social and employee-related matters affecting the company, respect for human rights, and handling of anti-corruption and bribery risks in their annual reports. These statements must include, among other things:
- a brief description of the company's business model;
- a detailed description of the internal policies on the above mentioned matters, including information on (due diligence and other) checks and processes implemented, and the results of these checks and processes;
- the main legal risks of the company in these areas, including a description of implemented or planned measures to mitigate such risks; and
- an outline of the key (non-financial) performance indicators for measuring the effectiveness of the implemented or planned measures.

In addition, Slovenian commercial companies (save for small and medium-sized companies) must in future include a corporate governance statement in their annual reports, *inter alia* containing a description of the company's diversity policy applied in relation to administrative, management and supervisory bodies – with regard to aspects such as age, gender and educational / professional background – and the objectives of the diversity policy, planned implementation measures and results in the relevant reporting period.

Compliance with these new requirements and the completeness of the relevant statements shall be checked by auditors, who shall comment on those aspects in their audit opinions.

Implications
Although some Slovenian commercial companies already include non-financial (corporate governance and other) statements in their annual reports, the newly adopted additional reporting requirements will likely lead to changes in the mindset of entrepreneurs in relation to certain aspects that are still partially underdeveloped in some companies and business sectors in Slovenia, such as sustainability of business operations, compliance and diversity / HR.

Other than that – and besides the expected increased level of awareness, transparency, responsibility and prosperity in relation to the above-mentioned "soft" areas of commercial companies' business operations – such changes should also foster the comparability of competing companies across the EU, enabling potential investors to make educated investment decisions based on reliable and comparable information in publicly available records.

Public disclosure obligations of companies in Turkey

Murat Kutluğ | Alara Baki

Companies operating under Turkish law are subject to registration and announcement to the relevant Trade Registries of Turkey and other public disclosure obligations.

Under the Turkish Commercial Code No. 6102 ("TCC") and other relevant legislation, limited liability companies and joint stock companies incorporated under Turkish Law ("Companies") are obliged to publicly announce and disclose certain transactions which may have positive or negative effects on public interest. The TCC regulates the rules broadly in order to protect the public interest. This article summarises Companies' material obligations under the principle of "public disclosure".

A. Registration at the Trade Registries and announcements to the public
Pursuant to the TCC, Companies are obliged to register certain corporate actions with the relevant Trade Registry of Turkey and to disclose such actions at the official Trade Registry Gazette. Actions which must be registered and disclosed are broadly defined and listed in the TCC and the official websites of each provincial Trade Registry. Transactions which must be registered and disclosed include, but are not limited to:
(i) any action in relation to the incorporation of Companies; (ii) all ordinary / extraordinary general meetings of joint stock companies; (iii) capital increase / decrease; and (iv) any change in representation.

If the relevant parties do not meet the registration and disclosure obligation under this principle within 15 (fifteen) days following the transaction day, the transaction is deemed null and void.

B. Independent audit and publicly disclosed information
Under the TCC, Companies subject to an independent audit are obliged to establish a website to publicly announce and disclose their corporate actions and transactions. Companies that satisfy two of the three following conditions (separately or together with their subsidiaries or affiliates) are subject to an independent audit: (i) Companies with active assets valued at TRY 40 million (approx EUR 10 million) or more; (ii) Companies with annual revenue of at least TRY 80 million (approx EUR 20 million) or more; and (iii) Companies with at least 200 employees. These conditions must be satisfied for two consecutive fiscal years. The obligation to set up a website starts in the following fiscal year.

Companies may fulfil the requirement to establish a website either by themselves or through official service providers called Centralised Database Service Providers (MTHS), which are licensed private legal entities for setting up and protecting contents to be published on the official websites of companies subject to independent auditing. Such company websites are also registered under the Central Registration Recording System of the Ministry of Customs and Trade (MERSIS) number of the relevant company under the public disclosure obligation of the Companies.

Certain contents which have to be continuously disclosed to the public through the company's website include: (i) Company's title, address, paid and unpaid capital, details of board of directors members for joint stock companies and managers for limited liability companies, as well as the details of the independent auditor; and (ii) information on the legal entities appointed as members of the board of directors for joint stock companies and as managers for limited liability companies, as well as information on the natural person representative of the legal entity.

Mandatory contents which have to be disclosed on the website for a minimum of six months include: (i) information regarding any lawsuit, legal action against or initiated by Companies; (ii) resolutions regarding the representation and binding of the respective company; (iii) resolutions regulating the principles of the acquisitions of newly issued shares; (iv) the acquisition of the company shares by a company from within the same group company and within the thresholds as stated under the related regulations; and (v) dominance agreements executed between Companies.

Members of the managing bodies of Companies who fail to publish and / or disclose the related content on their websites in due time may face monetary fines from 100 days to 300 days. In addition, persons who fail to duly disclose the relevant content will face fines up to 100 days. The fines are calculated based on daily income as subject to certain thresholds.

C. Public disclosure obligation in group companies
In line with other public disclosure requirements of Companies subject to the TCC (whether publicly held or not), the TCC regulates specific public disclosure obligations regarding the changes in shareholding structure of group companies. Group companies are defined as "a group of companies consisting of a controlling capital company and at least two capital companies controlled by such controlling company, whether directly or indirectly". The respective provision, Article 198 of the TCC, regulates the following:

• if a company acquires shares corresponding to 5%, 10%, 20%, 25%, 33%, 50%, 67% or 100% of the entire capital of a capital company or the respective shares fall under these percentages, the respective company has to notify the competent authorities with respect to the change within 10 days following the completion of the transaction. Accordingly, an announcement has to be made in the Trade Registry Gazette under the public disclosure obligation of the relevant parties;

• although the notification is made in a simple form, failure to notify shall have certain consequences on the relevant parties. In the event of failure to comply with the notification, registration and announcement obligations under Article 198 of the TCC, the shareholding rights, including the voting right pertaining to the relevant shares, shall be suspended until the full performance of the obligations. In the preamble of the law, the basis of the disclosure is set forth as a "public interest" and "public disclosure requirement."

D. Public disclosure platform
Under the Turkish Capital Markets Law No. 6362 ("CML"), starting from 1 June 2009, companies traded on capital markets and all brokerage houses are required to publicly disclose their financial statements, balance sheets, material events, explanatory notes and other notifications in a digital data collection system called the Public Disclosure Platform (Kamuyu Aydınlatma Platformu) operated by the Istanbul Stock Exchange. The main purpose of the CML is to efficiently protect the rights and benefits of the third party beneficiaries and to ensure the sustainability of the public interest. In the event of a failure to disclose the relevant information, the breaching parties must pay significant administrative fines.

> Limited liability companies and joint stock companies incorporated under Turkish Law are obliged to publicly announce and disclose certain transactions which may have positive or negative effects on public interest. The Turkish Commercial Code regulates the rules broadly in order to protect the public interest.

04 dispute resolution

Rules of Evidence vs Privacy

Commercial mediation – confidentiality matters

Anne-Karin Grill | Sebastian Lukić

International commercial mediation has become increasingly important in international dispute resolution. Commercial contracts now regularly contain business-friendly mediation clauses and the number of cases is on the rise.

A key element of mediation is confidentiality. When a neutral third person – the mediator – assists in commercial negotiations between the parties, open communication and disclosure of crucial aspects of the case are essential. Openness clearly increases the likelihood of a settlement.

Confidentiality is thus indispensable for every mediation process. Mediation is only an effective dispute resolution tool that parties benefit from fully if confidentiality is duly protected, both internally and externally. While the internal dimension of confidentiality concerns the disclosure of information between the parties and the mediator, the external dimension concerns the disclosure of information towards third-party entities, in particular courts and arbitral tribunals.

The internal dimension of confidentiality

As a matter of principle, the parties in dispute either explicitly or implicitly (by reference to institutional mediation rules) agree that the mediator shall be obliged not to disclose any information provided by one party in the absence of the other party, unless the party giving the information expressly waives such confidentiality towards the other party. A scenario where the mediator works with only one party at a time is commonly referred to as a "caucus". It is a procedural tool regularly applied by mediators. Caucusing requires a high level of integrity and an extensive obligation of confidentiality on the part of the mediator.

The external dimension of confidentiality

One of the main advantages of mediation is its compatibility with other dispute resolution methods. If the parties fail to reach a consensual solution and judicial or arbitral proceedings become necessary, confidentiality may become a source of further conflict. While mediation serves to achieve a negotiated settlement, litigation and arbitration allow a third party, be it a judge or an arbitrator, to decide which party will prevail. What is required is a process for establishing the relevant facts of the case. This, in turn, requires the disclosure of evidence. Critically, the parties

may be tempted to leak a document or other critical information that they obtained during a prior mediation process. At the same time, judges or arbitrators cannot simply cast a blind eye on confidential information unlawfully slipped into the proceedings. It is precisely because of this understanding of the judiciary's duties, at least in the civil law tradition, that the principle of confidentiality may be compromised. In fact, even if the parties explicitly agreed that information disclosed during the mediation process should be kept confidential, the effect of such protective measures is in no way absolute.

Notably, under the main legal framework for international mediation seated in the European Union – EU Directive 2008/52 on certain aspects of mediation in civil and commercial matters ("EU Mediation Directive") – and under the national laws implementing the EU Mediation Directive, confidential information is protected only insofar as testimonial evidence is concerned. The mediators and administrators of the mediation process cannot be compelled to give evidence in civil and commercial judicial or arbitration proceedings regarding information arising out of or in connection with a mediation process. This rule applies unless the parties agree otherwise, or if overriding considerations of public policy are concerned, or if disclosing the content of the agreement resulting from mediation is necessary in order to implement or enforce that agreement.

Accordingly, under Austrian law, mediators may refuse to testify before courts or tribunals if their testimony on a particular subject matter would violate their confidentiality duties under Section 3 of the Austrian EU Mediation Act (EU-Mediations-Gesetz) and Section 321 of the Austrian Code of Civil Procedure. However, while in certain jurisdictions parties may indeed be restrained by injunction from breaching a contractual confidentiality obligation and courts or arbitral tribunals cannot consider confidential information, Austrian law does not prevent parties from leaking confidential information obtained during mediation. Even if the confidential information is introduced into court or arbitration proceedings by a breach of confidentiality duties, the other party's hands are essentially tied. The only available remedy is a claim for damages for breach of contractually stipulated confidentiality.

Protecting confidentiality

Confidentiality is doubtless an important element of every successful mediation process and therefore requires careful protection. The parties in dispute will be willing to disclose information without risking their legal case being jeopardised in subsequent judicial or arbitration proceedings only in a confidential environment. The good news is that reports of cases where confidentiality was breached and confidential information was abused before a court or arbitral tribunal are very rare. Nevertheless, in addition to setting up a contractual framework that bolsters the protection of confidentiality, parties in mediation are also advised to pay particular attention to how they disclose information during the mediation.

> “Confidentiality is indispensable for every mediation process. Mediation is only an effective dispute resolution tool that parties benefit from fully if confidentiality is duly protected, both internally and externally.

Disclosure in Austrian civil proceedings


Maximilian Raschhofer | Michael Stimakovits

Evidentiary proceedings are at the heart of all litigation and form the basis of any judgment. Sometimes the evidence is not in the possession of the party wishing to rely on it. In common law jurisdictions, parties may base their cases on their own documents as well as those in the possession of their opponent, and may force their opponents to produce all relevant documents in a pretrial discovery procedure.

In civil law jurisdictions, however, the parties in litigation have rather limited procedural rights to request that their opponents produce evidence. However, the Austrian Code of Civil Procedure (CCP) also provides for legal instruments that may be used to force opponents (or third parties) to produce documents or physical items. Even if limited compared to other jurisdictions, the power of the Austrian tools of disclosure should not be underestimated.

Documents in the possession of the opponent

A simple pretrial discovery procedure allowing a party to obtain possibly admissible evidence from its opponent is alien to the Austrian law of civil procedure. Under certain conditions, however, Austrian civil procedure allows for the disclosure of documents which are not in the possession of the party wishing to rely on it to prove the facts alleged in its written or oral pleadings.
Under Section 303(1) CCP, a party alleging that a document material to prove its case is in the possession of its opponent may request the court to order the opponent to produce that document. For this to not degenerate into a fishing expedition, the requesting party must either produce a copy of the requested document or, if that is not feasible, echo the contents of the respective document as precisely and completely as possible in its request. In addition, all the factual allegations to be proven by the requested document must be pleaded, and the requesting party must inform the court of circumstances indicating that the document is indeed in the possession of the opponent (Section 303(2) CCP). An Austrian court will decide upon a request to order a certain document to be produced only after having heard the opponent.

If the court ultimately decides to order the opponent to produce the document, Section 304 CCP sets out specific circumstances in which it is strictly obliged to comply:

- if the opponent himself has referred to the requested documents to prove its allegations; or
- if the opponent is subject to an Austrian civil law obligation to produce the document (the obligation may be contractual or statutory, eg restitution of a lease agreement or promissory notes and receipts according to Sections 1426 and 1428 of the Austrian Civil Code); or
- if the requested document constitutes a joint document of the parties to the dispute (a document is a joint document if it was established to be used by either party as means of proof, or to influence or secure their legal relationship, eg the original copy of articles of association or an arbitration agreement).

As for documents other than those listed in Section 304 CCP, the party ordered to produce a document may refuse to do so by invoking any of the grounds for refusal under Section 305 CCP. More precisely, it may refuse to produce a document (i) if its content relates to family affairs; (ii) if the opponent's reputation is damaged by its disclosure; (iii) if the disclosure causes harm to the opponent or a third party, or even entails criminal prosecution; (iv) if its disclosure violates an officially recognised duty of secrecy or business secrets; or (v) if other compelling reasons exist which warrant a refusal of disclosure.

Physical items in the possession of the opponent

In respect of physical items which are in the possession of the opponent, the evidentiary rules on inspection refer to the above-mentioned rules of disclosure of documents (Section 359 CCP).

Documents in the possession of third parties

Pursuant to Section 308 CCP, third parties are obliged to produce a document only if (i) the third party is subject to an Austrian civil law obligation to provide the party tendering evidence with the document, or if (ii) the document, with a view to its content, is a joint document of the party tendering evidence and the third party concerned (see above). If these requirements are met, upon request of the party tendering evidence, the court may order the third party to produce the document at the expense of the party tendering evidence. Unlike with regard to the parties of the litigation, the CCP does not provide for any grounds for refusal with regard to third parties.

The court must hear the opponent as well as the third party before deciding on the request to produce a document. If the third party denies that it possesses the document, the party tendering evidence must also attest that the document to be produced is in fact in the possession of the third party. The decision ordering a document to be produced can be enforced by seizure or by imposing a penalty and, if such a payment cannot be obtained, by coercive punitive detention. If the party tendering evidence cannot attest to the third party's possession, it must initiate separate civil proceedings against the third party by filing an action for restitution of the document.

Physical items in the possession of third parties

Section 369 CCP refers to the rules for producing documents only with regard to physical items in the possession of the opponent. There is no such reference with regard to third parties. Therefore, the court cannot order third parties to produce physical items for evidentiary purposes.

Just how confidential is arbitration?

With courts worldwide shattering the common misconception that arbitration is intrinsically confidential, parties are left wondering: just how confidential is arbitration?

The answer is:

it depends.

Turn the page to read more

Victoria Pernt

As with most aspects of arbitration, confidentiality rests with the parties. Yet, many arbitration agreements do not address confidentiality, and parties often struggle to amend their arbitration agreements once a dispute has arisen and battle lines have been drawn.

In those cases, it is the governing arbitral law that, together with the applicable institutional rules, informs the scope of confidentiality covering that particular arbitration. The "confidentiality default" likely to apply under Austrian law is summarised below.

Arbitral proceedings and connected court proceedings may be private
Although Austrian statutory law does not contain any explicit provisions on the privacy of arbitral proceedings, such privacy is universally recognised and often implied in arbitration agreements. It is further fostered by Section 616(2) of the Austrian Civil Procedure Code ("ZPO"), which permits parties with legitimate interests to request exclusion of the public in court proceedings connected to arbitration. It is argued that since Section 616(2) ZPO provides for privacy in court proceedings connected to arbitration, privacy should be afforded, all the more, to arbitral proceedings themselves.

Awards may be (partially) published
Even without the other party's consent, a party may publish the ruling or a redacted version of the award, if not the entire award itself. The applicable institutional rules may also contain provisions on publication. The Vienna International Arbitral Centre, for instance, may publish anonymous summaries or extracts of awards, unless the parties object.

Arbitrators are subject to a confidentiality obligation
Confidentiality obligations of arbitrators are universally recognised. They are derived from the contractual duty of care, laid down in guidelines and codes of ethics, and often implied in arbitration agreements. Arbitral institutions are generally under a similar obligation.

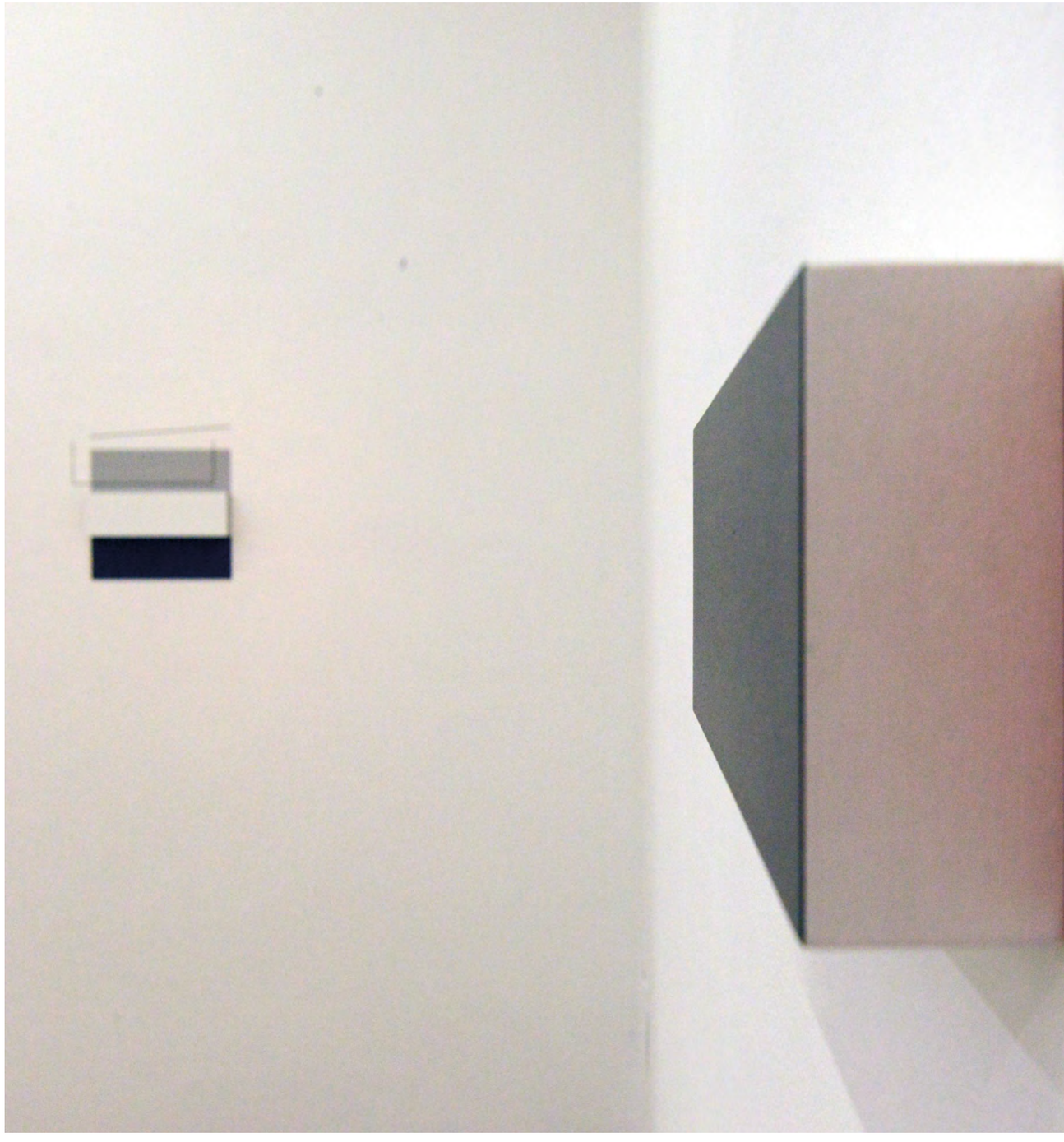
Parties may be subject to a (limited) confidentiality obligation
Neither Austrian statutory law nor case law expressly provides for a general duty of confidentiality. However, such a duty may be implied in Austrian law. Under Section 172(3) ZPO, if the public is excluded from a hearing, the content of that hearing may not be made public. Section 616(2) ZPO permits such exclusion of the public in the arbitration context. Therefore, it can be argued that Austrian law supports a general duty of confidentiality of the parties to an arbitration.

Nevertheless, even if such a duty existed, it would be subject to certain limitations. It would not prohibit disclosures required by law, challenges or enforcement of the award, or seeking assistance from courts in the course of the arbitration. It also would not prohibit disclosures to a smaller and closed group (such as potential purchasers), as only publications to "the public" are prohibited. Nor would such a duty prohibit the disclosure of at least the ruling of the award or a redacted version of it.

Can parties make their arbitration more confidential?
Yes, parties can and do influence how confidential their arbitration is. For one thing, parties should consider their confidentiality preferences when choosing the applicable institutional rules and governing arbitral law. The confidentiality provisions vary greatly by country. For example, the arbitral laws of New Zealand, Spain, England, France and Singapore recognise a general confidentiality obligation of the parties, while those of Australia, Sweden and the US do not. Naturally, choosing the right institutional rules and arbitral law requires sufficient familiarity with their respective key provisions.

Parties also can (and should) enter into confidentiality agreements. While confidentiality may at times be implied in a particular contract, relying on an implied obligation is hardly a risk worth taking. Parties are thus well advised to carefully draft tailored confidentiality provisions together with their arbitration agreement. For instance, these provisions could require that documents exchanged in the arbitration remain confidential, that witnesses and experts testifying in the arbitration sign confidentiality clauses, and, crucially, could subject breaches of confidentiality to contractual penalties.

Arbitrations, at least if seated in Austria, are likely to be more confidential than state court proceedings, even without particular confidentiality agreements. Nevertheless, parties are well advised to take the reins and include confidentiality provisions in their arbitration agreements. After all, it is up to them to determine just how confidential their arbitration will be.



Moving ahead on international dispute resolution

Dr Alice Fremuth-Wolf,
Secretary General of the Vienna International Arbitral Centre.

An interview by Anne-Karin Grill

Arbitration is a process designed to support the swift and effective resolution of disputes between commercial parties in a private forum. Schoenherr partner Anne-Karin Grill sat down with the Secretary General of the Vienna International Arbitral Centre (VIAC), Dr Alice Fremuth-Wolf, to discuss her institution's policies and to get her outlook on the future of international dispute resolution.

Q: Confidentiality and transparency are two key aspects of arbitration that are often mentioned in the same breath. Is this a contradiction?
A: There is a natural and intrinsic tension between transparency and confidentiality, but I would not go so far as to call it a contradiction.

One of the main features of commercial arbitration has always been its confidential nature. This allows parties to have their disputes settled in a private arena, which is perfectly fine.

To me, transparency is of utmost importance to prevent arbitration from being stigmatised as "jurisdiction behind closed doors", where decisions are being rendered that impact the fate not only of the parties but of a large group of people or even nations. This is especially so in investment arbitration cases. But major steps have already been taken in this respect (UNCITRAL Transparency Rules 2014).

This is not necessarily the case in commercial arbitration between two private parties, however, unless perhaps public legal entities are involved. There is no subordinate public need that their private disputes be publicly debated or commented. There should not be a spill-over effect from investment arbitration to commercial arbitration in these cases. If we move one step further to other forms of ADR, such as mediation, no one has ever doubted that the confidentiality of the process is critically important. In fact, it is an indispensable element for the parties to open up and find creative solutions without prejudice.

Arbitral awards are only published if there is an agreement between the parties to that end. Sometimes they are published in anonymised form. Do you consider this a "lack of transparency" and therefore as a problem for arbitration?
As I already mentioned, this is another area of tension between transparency and confidentiality. In my opinion, the publication of awards in anonymised form tries to strike this balance, as it allows the public to be informed about the outcome of a dispute providing a summary of legally relevant and interesting details to a greater audience, while cutting out confidential data and information that is superfluous.

According to Art 41 of our Rules of Arbitration, anonymised summaries or extracts of awards may be published in legal journals or the VIAC's own publication, unless a party has objected to the publication within 30 days upon service of the award. When the VIAC for the first time published its "Selected Arbitral Awards, Vol 1" in 2015, we prepared abstracts for each case part of this publication. As a matter of courtesy, we sought permission from the parties beforehand and were prepared to amend the drafts in accordance with the parties when they felt that the information disclosed could infringe their rights or lead to the parties being identified. With this admittedly cumbersome procedure, we ensured that interested parties felt safe while at the same time satisfying the appetite of practitioners to get insights into decided cases and their reasoning.

Your institution, the Vienna International Arbitral Centre (VIAC), has recently implemented some amendments. What are they about?
Our last big rules revision was in 2013, when we introduced several important new features, such as expedited proceedings, third-party joinder, consolidation and others.

In 2016, we revised our conciliation rules and created brand-new state-of-the-art Mediation Rules that enable us to administer ADR proceedings as well as ArbMedArb proceedings, which is a unique feature (only the SIMC and SIAC offer a similar system).

The new (still draft) 2018 Rules of Arbitration and Mediation will foresee the following new provisions without changing the content of the 2013 and 2016 rules:
- administration of purely domestic cases when parties have so agreed;
- security for costs provision;
- rules for tribunal secretaries;
- more flexibility in cost decision of arbitral tribunals in that also the behaviour

of parties and their counsel may be taken into account;
• more flexibility of the Secretary General when deciding on the fees for arbitrators in that behaviour will be taken into account (up to 50% premium in complex cases and/or when arbitration was conducted efficiently, as well as deduction of up to 40% in case of severe delays or any other behaviour of an arbitrator that would justify such reduction).

Can you name any concrete measures that the VIAC is taking in the interest of increasing transparency?
As of 1 September 2017, the VIAC has decided to publish the names of arbitrators acting in current proceedings. With this new initiative, the VIAC is making international arbitration easier to understand following the call for more transparency in the appointment process of institutional arbitration. The list will be updated regularly and provides information on the appointment method, ie if the arbitrator has been appointed by the board of the VIAC or nominated by the parties / coarbitrators, and the date when the case file was handed over to the respective arbitrator. It also shows if the case is still pending or if an arbitrator's office was prematurely terminated without stating the reasons.

We see this as an important step to show that diversity is already present and applied on an institutional level in the selection of arbitrators as regards gender, age and nationality. We hope this also serves as a benchmark for parties when they choose their arbitrator, where there is still room for improvement. The fact is that diverse tribunals work better and arrive at more balanced and better solutions.

Where do you see the greatest challenges for commercial arbitration in the future?
I think the biggest challenge is that arbitration runs the risk of suffering the same fate as litigation and thus be replaced by other means of ADR, such as mediation. In our quest to monitor, control and develop, we have reached a point where the once flexible instrument of arbitration has become over-regulated by rules, guidelines, notes and codes of conduct.

Some critics argue that arbitration stifles the development of state court jurisprudence, since some areas of law are effectively monopolised by arbitration. What is your position?
I think that there is a reason why parties have turned their backs on state court litigation and resorted to arbitration in some areas (eg m&a). One may be the selection of the arbitrators, which ensures that specialised persons deal with the disputes instead of state court judges, to whom cases were assigned randomly. Another may be the confidential nature of the proceedings.

In civil law countries, the law should not be made by judges, but by the parliament. But even if there is no binding case law, Supreme Court judgments still serve as an important guide, as they are publicly available. Of course, this argument alone should not suffice to criticise arbitration, as this development is not its fault. Solutions should be found for the underlying need, ie the availability of decisions in certain areas.

I am convinced that the publication of abstracts of awards in certain areas where parties have shied away from state court litigation would help to ensure the availability of sufficient case law in certain areas, even if non-binding.

The VIAC is the leading arbitration institution in Central and Eastern Europe. Why should the users of dispute resolution services choose the VIAC?
This is easy to answer: Because we have been active in this market for more than 40 years and have perfect knowledge of the players, parties, potential arbitrators and their specific needs and expectations. Our experience in this region is unmatched. We are often seen (and actually are) a common denominator and neutral ground for East-West disputes in the broadest sense, also encompassing disputes between parties from Asia and Europe.

Thank you for the interview.

> “As of 1 September 2017, the VIAC has decided to publish the names of arbitrators acting in current proceedings. With this new initiative, the VIAC is making international arbitration easier to understand following the call for more transparency in the appointment process of institutional arbitration.

05 eu & competition

How Do Privacy Rules Limit Anti-Trust Investigations

Competition law and privacy can collide in several ways, whether by competition authorities interfering with the right to privacy in their investigations, or by companies seemingly caring little about consumers' privacy interests owing to their market power.

Mariella Friedrich

1. The fundamental right to privacy in competition investigations – effective protection or lip service?

Most competition authorities can raid businesses and private premises in order to obtain documents that evidence presumed infringements of competition law. They have the power to conduct "all necessary inspections", meaning that the investigation decision must be based on reasonable grounds and aimed at verifying the existence and scope of a presumed infringement based on already available information. Fishing expeditions are not allowed.[1]

1.1 Fundamental right to data protection in antitrust investigations – "E-discovery" in the course of dawn raids and related problems regarding seized private data.

The right to privacy, which comprises the right to data protection, is especially at risk when competition authorities examine virtually the entire IT environment of an undertaking. When sifting through hardcopy documents, a quick look at the document often allows the investigator to identify whether it is exempted from review. This does not hold true for masses of digital information seized and later examined by the authority, leading to a critical tension between "e-discovery" measures and the right to data protection.

The Volker and Markus Schecke GbR / Land Hessen[2] case would suggest that the right to data protection only applies in a very restricted way to legal persons.

* Footnotes on page 68

However, the right to data protection of natural persons also can be affected, especially the "blind" confiscation of whole mailboxes, which can include private correspondence. While it has been confirmed that an ediscovery as such does not violate the right to privacy,[3] such measures have to be proportionate. Confiscation of masses of electronic data which include private data is thus only admissible if (i) the confiscation itself is related to the alleged infringement and not arbitrary (eg restricted to the employees working in the field of the activity concerned); (ii) the investigated undertaking is provided with a copy as well as a report of the seized data; and (iii) the authority was not able to filter the seized data more stringently. The technological possibilities of further selection will therefore be decisive for the legality of e-discovery measures.[4] Widespread and indiscriminate confiscation of IT data is prohibited. The undertaking must also have the possibility to object to the confiscation.

1.2 Effective protection?
At the EU level, an investigation decision of the European Commission ("EC") as such can be challenged before EU courts. However, if disproportionate measures infringing fundamental rights arise in the course of the inspection itself, no separate action is possible, but it constitutes a part of the review of the EC's final decision by EU courts. As the EU is not yet itself a member of the European Charter of Human Rights ("ECHR"), an application to the European Court of Human Rights ("ECoHR") against actions of the EC is not possible. In contrast, undertakings can make an application against infringements of fundamental rights through actions of Member States or their representatives to the ECoHR after having exhausted all national remedies.

Overall, in recent years the EU courts have recognised a number of fundamental rights relevant to the enforcement of competition rules, and are placing ever greater emphasis on the compatibility of competition procedures with the EU Charter of Fundamental Rights, the ECHR and the jurisprudence of the ECoHR. Still, one can question whether the possibility of reviewing the legality of dawn raids only *ex post* provides sufficient protection. After all, authority officials will gain knowledge from the reviewed data even if the review is subsequently found to be illegal.

The current belief, though, is that the protection measures in place against antitrust investigations of the EC strike an acceptable balance between the right to privacy and effective investigation measures. Still, several areas remain where the relationship between effective protection of the right to privacy on the one hand and effective enforcement on the other hand seems grossly unbalanced. For example, at the EU level, enforcement trends in merger control proceedings risk undermining fundamental rights. At the national level, several national regimes or enforcement practices of national authorities in Central and Eastern Europe seem at odds with the EU case law on fundamental rights, even in the area of antitrust investigations.

“
The current belief, though, is that the protection measures in place against antitrust investigations of the EC strike an acceptable balance between the right to privacy and effective investigation measures.

2.
The Delta Pekárny case as a leading example of ineffective protection in an Eastern European Member State?

Claudia Bock

2.1 The practice of the Czech Competition Authority in question.
The legality of a 2003 dawn raid carried out by the Czech Competition Authority ("CCA") on Delta Pekárny's business premises was the subject of a long-running dispute. The CCA has the power to inspect business premises without any prior judicial warrant (a court order is only needed to inspect private premises). Czech procedural law afforded the implicated companies two procedural options to challenge the legality of the raid – one requiring the CCA to terminate the administrative proceedings without finding an infringement, the other requiring the company to await the final decision on the infringement. In 2014, the ECoHR found such an *ex-post* review to be ineffective, since it is not sufficiently immediate.[5] As a consequence, the Delta Pekárny dawn raid was considered illegal. Also, the review of the case before the Czech Constitutional Court was re-opened.

2.2 Immediate consequences of the ECoHR decision – bringing dawn raids to a temporary halt.
The ECoHR decision was a significant blow to the CCA. It put all planned dawn raids on hold for several months in order to evaluate the judgment and to look for a solution in order to resume dawn raids. The initial understanding of the CCA after the ECoHR decision was that the CCA could perform dawn raids only with prior judicial approval, unless a legislative change was made. At the beginning of 2015, the tide turned and the CCA resumed dawn raids, claiming that the CCA's analysis showed that no prior judicial approval would be necessary. The Delta Pekárny judgment was believed to be an isolated one based on several peculiarities of the case without the possibility or need to infer general conclusions, and the CCA did not identify a systemic problem in the Czech legal system. The CCA claimed that the legal system offered sufficient immediate legal protection to challenge the legality of a raid, particularly through a specific administrative action (the so-called action against illegal interference of an administrative body, "separate administrative action"). However, the case law and legal interpretation at that time allowed such an action to be filed only if a final decision on the infringement was issued.

2.3 The decision of the Czech Constitutional Court and legislative changes.
In the re-opened case on the Delta Pekárny dawn raid, the Constitutional Court considered the raid illegal in February 2016, siding with the ECoHR that the Czech legal system afforded insufficient protection of fundamental rights.

In order to bridge the legal uncertainty after the statements of the CCA and the decision of the Czech Constitutional Court and to guarantee sufficient immediate protection of fundamental rights in compliance with EU requirements, changes were introduced in the applicable legislation whereby it was explicitly stated that any company can file a separate administrative action to challenge the legality of a dawn raid. The separate administrative action must be filed within two months of the inspection, irrespective of the status of the infringement proceeding.

“
...changes were introduced in the applicable legislation whereby it was explicitly stated that any company can file a separate administrative action to challenge the legality of a dawn raid.

3.
Does the right to privacy play any role in merger control proceedings?


Franz Urlesberger | Lukas Solek

One might be surprised to read that data protection rules might also impact the competitive assessment of a concentration within merger control proceedings. Nonetheless, the clash of these two universes can be increasingly seen with respect to mergers pertaining to the digital sector. The most recent example is the EC's probe of the VERIZON/YAHOO deal.[6] Both Verizon and Yahoo used certain data generated by user activity on their websites, apps and other services such as their ad networks to improve their online advertising services (eg sold to advertisers and publishers) and better target advertising on websites and apps.

The EC saw two potential issues concerning these online advertising services as a result of the combination of the two datasets previously held independently by Verizon and Yahoo: (i) the increased market power of the merged entity; and (ii) the elimination of competition based on the data that existed between Verizon and Yahoo prior to the merger.

> While data protection rules play an increasingly important role in assessing concentrations in the digital sector, there is a general worry as to whether the EC gets to assess such concentrations in the first place.

In the end, the EC has not deemed this combination of datasets to raise serious competitive concerns. One of the notable reasons for this conclusion was the applicable data protection regime. The EC noted that any combination of the said datasets could only be implemented to the extent allowed by applicable data protection rules. Both Verizon and Yahoo were subject to such rules with respect to the collection, processing, storage and usage of personal data, which, subject to certain exceptions, limit their ability to process the datasets they maintain.

The EC also took account of the newly adopted General Data Protection Regulation ("GDPR") which would limit the parties' ability to access and process users' personal data in the future, since the new rules will strengthen the existing rights while giving individuals more control over their personal data (ie easier access to personal data, right to data portability, etc).[7]

Another recent example of data protection rules coming into play within the competitive assessment came to light during the EC's assessment of an envisaged joint venture between Sanofi and Google.[8] The joint venture was meant to offer services for the management and treatment of diabetes, including data collection, processing and analysis. In its competitive analysis, the EC addressed concerns voiced over the ability of the parties to lockin patients by limiting or preventing the portability of their data towards alternative services.

The Commission dismissed these claims by *inter alia* pointing to the GDPR, which will provide the users with the right to request portability of their personal data. Data subjects have the right to receive a copy of their data in a structured and commonly used machine-readable format, as well as the right to transmit their data to another controller or to request the controller to transmit their data directly to another controller. In light of this, the EC considered the power of locking-in patients to the services of the joint venture to be unlikely in the foreseeable future.[9]

While data protection rules play an increasingly important role in assessing concentrations in the digital sector, there is a general worry as to whether the EC gets to assess such concentrations in the first place. In its recent opinion, the European Data Protection Supervisor noted that the EU merger control rules focus on companies which meet certain turnover thresholds, unless cases are referred by national competition authorities. Nonetheless, there are indications that proposed acquisitions of less established digital companies, which may have accumulated significant quantities of personal data that have yet to be monetised, will face greater scrutiny.[10] However, such acquisitions can normally only be caught by merger control rules if alternative means of establishing jurisdiction, such as transaction value thresholds, are introduced. Such rules have already been adopted in Germany and Austria. The future will show whether the EU will follow this approach and what role data protection will assume within the competitive assessment of concentrations in the years to come.

4.
Privacy rules and competition law enforcement

Christoph Haid

The economic value of data as an input has been considered and acknowledged widely by competition authorities when reviewing concentrations in the digital industry. Several transactions have been assessed against whether the acquirers would derive market power from gaining access to the data troves of the target companies. As to privacy considerations, the EC stated in Facebook / WhatsApp that "even if there might be concerns that the concentration of data within the control of Facebook post-merger might impact privacy, respective concerns are outside the scope of competition law and should be dealt with by [appropriate] protection rules."[11] In Asnef Equifax, the ECJ found that "…issues relating to the sensitivity of personal data are not, as such, a matter for competition law, [but] … provisions governing data protection."[12]

One would be mistaken to conclude that there is no intersection between data protection rules and competition rules. Commissioner Almunia already pointed out in 2012 that "a […] dominant company could […] think to infringe privacy laws to gain an advantage over its competitors."[13] The debate over the relevance of data protection for competition law has intensified significantly since then.

Besides data protection being a fundamental right that every competition authority needs to respect, stricter data protection rules are believed to facilitate customer choice and ultimately benefit consumer welfare, which is at the heart of competition policy. Proponents of giving more weight to privacy considerations in antitrust assessments claim that privacy rules are a significant aspect of the quality of (often free) services offered by the digital industry, valued highly by consumers, but treated sluggishly by the dominant players owing to the power imbalance between the former and the latter. The more powerful the company in the digital industry, the more the level of data protection is believed to be at risk, with authorities being ill-equipped to assess these issues with their current economic toolset. Antitrust policy should actively encourage privacy competition, because high entry barriers due to several data-driven network effects and the incumbent's behaviour prevent the emergence of competing service providers that offer better privacy policies.

Those who argue against giving privacy considerations more room in antitrust enforcement point to three aspects: (i) the relevance of a company's privacy policy as a dimension of the quality of its service is overrated in light of customers' relaxed approach to such policies; (ii) it follows from the decisional practice that customers' claims of being locked-in to a dominant provider to the detriment of alternative providers is invalid as long as switching is feasible, owing to the relevant data being available; and (iii) if competition law would have to ensure effective privacy, this would not only mean a departure from the standard analysis of efficiency, but would open the door for any other fundamental right or public policy having to be considered by antitrust enforcers. Such a result would lead to greater uncertainty over competition law enforcement, whereas the recent legal developments equip data protection authorities with a sufficient deter-

rent to combat lopsided relationships between individuals and the data controller.

In light of this, there is a lot of anticipation about the outcome of the pending investigation by the German Federal Cartel Office against Facebook over an alleged abuse of dominance. Assuming Facebook is dominant (which the FCO first needs to establish in its investigation, which seems difficult), the authority is looking into the question of whether disregarding customers' privacy interests and making access to the social network conditional upon accepting Facebook's privacy policy constitutes an abuse. It will be fascinating to see whether the authority will deploy an analytical approach based on standard economic efficiency (so that an abuse would only be established if the practice were to lead to an increase in prices or decrease in quality, which is not outweighed by other efficiency gains) or actually opens the door so that violations of data protection rules would be firmly included into the substantive assessment of competition rules.

> One would be mistaken to conclude that there is no intersection between data protection rules and competition rules.

1 ECJ, Case C583/13 P, Deutsche Bahn AG v Commission EU, paras 1836.

2 ECJ, Case C92/09 and C93/09, Volker and Markus Schecke GbR/ Land Hessen, paras 53 and 54.

3 GC, Cases T135/09, Nexans, and T140/09 Prysmian; ECoHR, Cases Robathin v Austria and Vinci v France.

4 However, as Judge Zupancic stated in his concurring opinion in Vinci v France, it will often be hard to prove whether or not further technological selection possibilities existed. See also Seelos /Harsdorf, Veni, vidi, VI(N)CI? Der EGMR und die elektronische Datensicherung im Rahmen kartellrechtlicher Hausdurchsuchungen in Frankreich, ÖZK 2015, 149.

5 Delta Pekárny A.S. v. Czech Republic, App. No 97/11, ECHR 279, Judgment of 2 October 2014 (NYR).

6 COMP/M.8180 – VERIZON/YAHOO, rec 80 et seq.

7 Also see COMP/M.8124 – Microsoft/ LinkedIn, rec 167 et seq; the EC recently used similar reasoning in COMP/M.8251 BITE/TELE2/TELIA LIETUVA/JV, rec 85 et seq, with respect to data collection on customers within the provision of mobile payment services.

8 COMP/M.7813 SANOFI/GOOGLE/ DMI JV, rec 63 et seq.

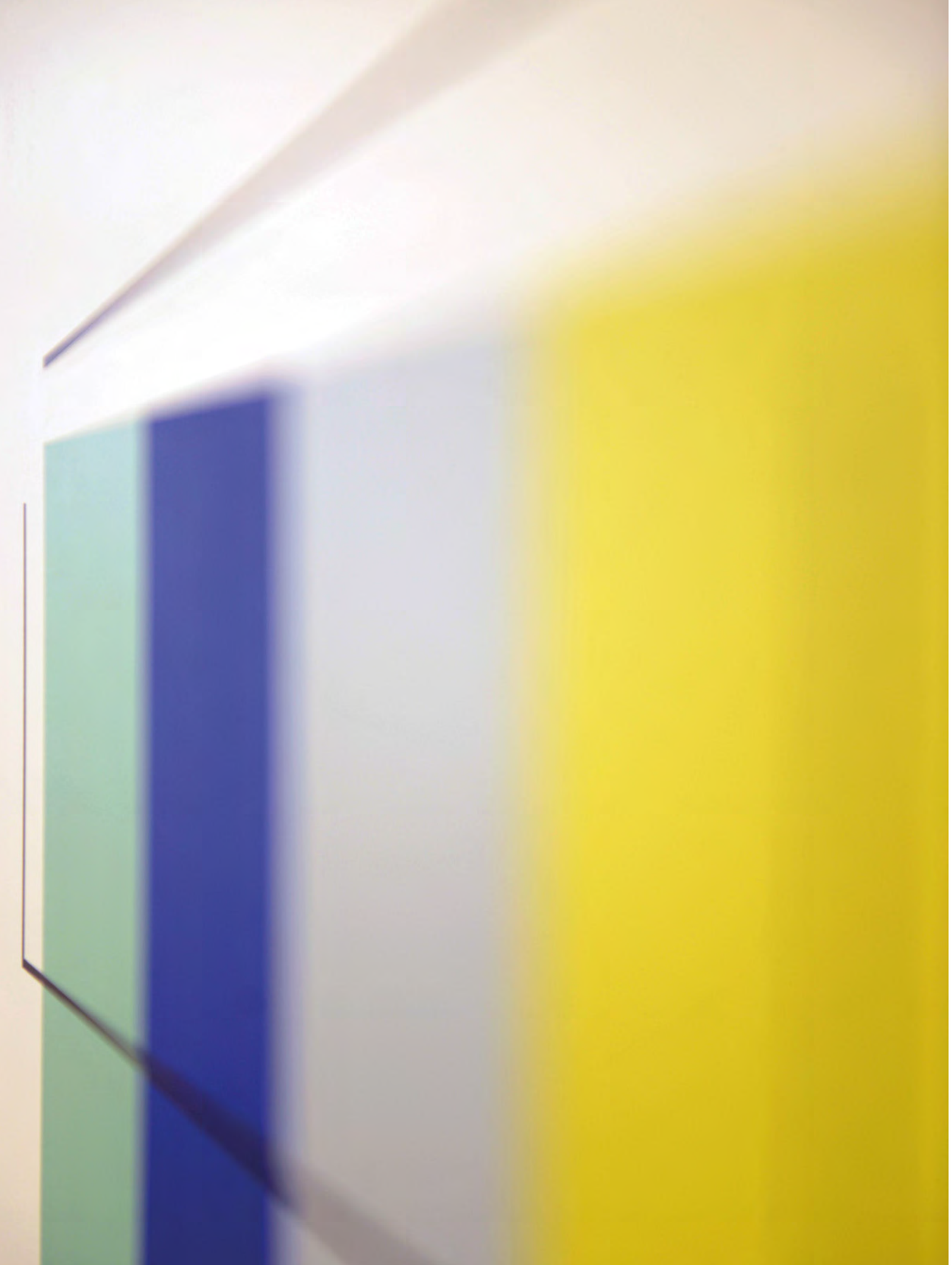
9 Also see COMP/M.7337 IMS HEALTH/CEGEDIM BUSINESS, rec 218.

10 European Data Protection Supervisor, Opinion 8/2016 of 23 September 2016, EDPS Opinion on coherent enforcement of fundamental rights in the age of big data, p 14 et seq.

11 COMP/M.7217 – Facebook/Whats-App, rec 164.

12 Case C238/05, AsnefEquifax v Asociación de Usuarios de Servicios Bancarios, rec 63.

13 Joaquín Almunia, Competition and personal data protection – Speech at Privacy Platform event on Competition and Privacy in Markets of Data (26 November 2012), available at www.europa.eu/rapid/pressrelease_ SPEECH12860_en.htm



06 insolvency & restructuring

Confidentiality in Restructuring

Confidentiality in restructuring

> All information relevant for the restructuring must be available to the creditors, and must be kept confidential.

Wolfgang Höller | Miriam Simsa | Philipp Wetter

Successful restructurings typically depend on a smooth and swift process. All information relevant for the restructuring must be available to the creditors, and must be kept confidential. In addition, legal duties of secrecy must be considered. Finally, the effective restructuring of a debtor's business needs to receive as little attention as possible from third parties (eg customers, the market, suppliers).

Information is key

Receiving timely and transparent information about all circumstances relevant for the restructuring process is crucial for the decision-making of the creditors involved. Creditors usually require comprehensive information on the assets, liabilities, granted securities as well as the business of the debtor and on any proposed restructuring measures. In addition, the banks have to be released from their duties under banking secrecy towards other creditors. Without full transparency and sufficient information, no creditor will ever trust the debtor and the other creditors enough to agree to an often painful restructuring.

So is confidentiality

A debtor will only consent to disclose sensitive information about its business to its creditors if it is certain that the information will be kept strictly confidential. Apart from the economic impact, management and the shareholders often want to avoid the stigma of a failing business.

Also, creditors have a vital interest in making sure that the process does not become public. Customers may avoid buying from a distressed seller, suppliers may deliver only against advance payment, and a prospective buyer in an m&a process may reduce its price offer if it learns that the debtor is compelled to sell a certain business. All of this may significantly impair the creditors' prospects of recovery.

In short, leaking information may be so detrimental to the debtor's business that the restructuring itself becomes impossible.

Keeping information confidential is difficult in a multiparty process. As it is in their best interest, creditors and debtors still have to try.

Outlook

Recently, the European Commission published its proposal for a European Directive on preventive restructuring frameworks and a second chance for entrepreneurs. More and more states are aiming to implement a legal framework which allows preventive restructuring proceedings.

One of their main benefits is to avoid the stigma of insolvency as well as publicity. The European legal framework currently only allows the recognition of public, collective (insolvency) proceedings initiated in other Member States. National laws on preventive restructuring proceedings will have to address the need for publicity.

At the European level, it should be ensured that preventive restructuring proceedings limiting publicity to a minimum will be recognised in all other Member States.

07 ip, it & life sciences
Trade Secrets

Is trademark a celebrity's best friend?


Eva Škufca | Urša Kranjc

Many celebrities are choosing to register their names as a trademark in order to prevent other people from exploiting it for profit (ie advertising products carrying their names). One could argue this basically means that they seek for privacy through trademark registration, which is rooted in the idea that everyone should have the right to be left alone and have control over the commercialisation of their persona, including celebrities, who have invested a lot of work in building their recognition in the world of fame.

We talked about this with rising young football star Carlos Rolando*, who was seeking advice on protecting his privacy through trademark registration.
* The interviewee is a fictional character who we created for this contribution. His trademark rights have not (yet) been protected.

Why do celebrities trademark their personal name?

After a great season in the Football Kings League, Carlos Rolando's name exploded like a bomb. In a world of Twitter, Facebook and Instagram, there are not many left, who would not recognize his name. Moreover, he has recently become aware of many products, such as T-shirts, cups, perfumes and even dog collars bearing his name. He pointed out that these products create confusion among customers, who probably believe he is endorsing them, which is not the case. Taking into account his charity endeavours, he also does not want anyone to be able to benefit from his name for commercial purposes only. He wants to be a football player first and foremost, not a celebrity, and therefore wishes to register his name as a trademark to prevent such exploitation.

Grounds for registering a personal name as a trademark in the EU

Under Regulation 2015/2424,[1] an EU trademark may consist of any signs, in particular words, including, inter alia, personal names, provided they are capable of distinguishing the goods or services of one undertaking from those of others.[2]
A trademark does not give a celebrity all-encompassing rights to his or her name, but is limited to the indication of origin of the goods and services, which is the trademark's function. Therefore, if

successfully registered, the celebrity gains a monopoly on his or her name only for registered goods and services.

Carlos was thus advised to select the most appropriate classes of goods and / or services when registering the trademark. For example, it does not make much sense to register a "Carlos Rolando" trademark for chemical products (Class 1 of NCL[3]) or motors and engines (Class 7 of NCL), but certainly does when it comes to things like clothing, footwear (Class 25 of NCL) or toys (Class 28 of NCL).

Downside of trademarking a personal name

During our talk, Carlos emphasised that he only wants to prevent third parties from exploiting his name for profit and has no intention of using the "Carlos Rolando" trademark himself as he only seeks for some privacy. This sounds reasonable enough, but is not how the world of trademarks works. If a celebrity wants to keep the trademark, he or she will have to use it; otherwise it may be subject to revocation.

Under Regulation 207/2009,[4] the rights of the proprietor of an EU trademark can be revoked if the trademark has not been put to genuine use in the EU in connection with the goods or services in respect of which it is registered within a continuous period of five years and there are no proper reasons for non-use. Moreover, where grounds for revocation of rights exist in respect of only some of the goods or services for which the EU trademark is registered, the rights of the proprietor shall be declared revoked in respect of those goods or services only.[5]

This means that in order to keep his trademark, Carlos will need to "start a career" in relation to registered goods and services, otherwise he may "lose" his privacy in respect of some or all of the goods or services for which the trademark is registered. For example, to prevent third parties from producing and selling T-shirts, sweaters and other clothing, Carlos will need to start his own clothing line to keep his trademark safe.

Conclusion: friendly, but not a friend

Registering a personal name as a trademark is a double-edged sword. It may prevent others from exploiting a celebrity's name, but in order to preserve the situation, the celebrity has to use the trademark. This forces celebrities to engage in different businesses in return for privacy.

In the middle of our discussion, Carlos Rolando asked: "Does trademark registration of my personal name even protect my privacy or only let me choose who will exploit and commercialise my name?" Good question! Now he knows the answer.

> “ Registering a personal name as a trademark is a double-edged sword.

1 REGULATION (EU) 2015/2424 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 December 2015 amending Council Regulation (EC) No 207/2009 on the Community trademark and Commission Regulation (EC) No 2868/95 implementing Council Regulation (EC) No 40/94 on the Community trademark, and repealing Commission Regulation (EC) No 2869/95 on the fees payable to the Office for Harmonisation in the Internal Market (Trademarks and Designs) ("Regulation 2015/2424").

2 Art. 1, para. 8.

3 The Nice Classification ("NCL") is an international classification of goods and services applied to the registration of trademarks.

4 COUNCIL REGULATION (EC) No 207/2009 of 26 February 2009 on the Community trademark ("Regulation 207/2009").

5 Article 51.

Statutory secrecy obligations related to employee inventions in Austria and Romania


Eduard Pavel | Adolf Zemann

Secrecy plays a pivotal role in the area of patent law. The disclosure of an invention before a patent application has been filed can destroy novelty and therefore patentability, even if the disclosure is made without the inventor's consent. Accordingly, patent laws often provide specific rules on non-disclosure, in particular within the context of inventions made by employees.

This article provides an overview of these rules in Austrian and Romanian patent law.

Austria

Under Austrian law, an employee can only assign rights to future inventions to his/her employer if the inventions are considered employee inventions within the scope of the Austrian Patent Act ("APA"). A written agreement, eg in the employment contract or in the form of a collective bargaining agreement, is necessary. If such an agreement exists, the employee has to report any invention made to the employer, unless it is evidently not covered by the agreement. The employer must declare within four months of the report (shortened to three months in many collective bargaining agreements) that it claims the invention, otherwise it belongs to the employee.

To safeguard the interests of both the employee and the employer, in particular within this period of uncertainty as regards who will own the invention, the APA provides specific secrecy obligations:

• as a general rule, employees and employers are obliged to keep the invention covered by the above-mentioned report and declaration;
• the employee's secrecy obligation under this provision ends:
- if the employer does not claim the invention in time; or
- if the employer claims the invention in time, but abandons secrecy (of course, the obligation also ends if the employer publishes a patent application, insofar as the invention is disclosed in the published patent application).

Any other secrecy obligations imposed on the employee (either contractually or by law) remain unaffected.
• The employer's secrecy obligation ends if it claims the invention in time and the employee does not object to this claim (the employee might object that the invention is not an employee invention within the scope of the APA and that the rights in the invention therefore belong to him).
• The secrecy obligations do not prevent the employer and the employee from taking the necessary steps to safeguard their rights in the invention, in particular to apply for a patent.
• Any breach of this secrecy obligation gives rise to claims for damages of the other party, which also covers lost profits.
• The rights and obligations conferred to the employee and the employer remain intact even after the employment relationship has ended.

Romania

Romanian Law 83/2014, on Employees' Inventions ("LEI") differentiates between inventions created by employees as part of an inventive mission expressly assigned by the employer (inventions with an inventive mission) and inventions created by employees in the absence of an inventive mission (inventions without an inventive mission).
• The right in employee inventions with an inventive mission belongs to the employer. If the employer is a legal person under public law in the field of research and development, contractual provisions may provide that the right belongs to the employee.
• The right in employee inventions without an inventive mission belongs to the employee if the employer does not claim the invention within four months after it has been communicated to the employer or a longer period is stipulated under the employer's internal regulation.

In addition, the LEI provides for the following secrecy obligations in regard to employee inventions, regardless of which of the above-mentioned categories they fall under:
• the LEI clarifies that employee inventions may be subject to trade secrets;
• the employee-inventor shall not disclose or publish the employee invention without the employer's written consent. The same applies to the employer and to any third parties that learned of the invention due to the nature of their work;
• failure to comply with this secrecy obligation
- triggers liability under the employment contract, if it contains a non-disclosure clause; or
- if no such non-disclosure clause is provided for, where damage results from the disclosure, may trigger the tort liability under the provisions set forth by the Romanian Civil Code.

These examples show different approaches to regulating secrecy obligations in relation to employee inventions. Beside these rules under employee inventions law, Austrian and Romanian law also provide specific rules on the use of trade secrets (employee inventions will often be considered trade secrets).

A certain harmonisation of these rules is to be expected due to the trade secrets directive.

How to obtain formal design protection for your catwalk designs and still keep them secret

Denisa Assefová

A so-called deferment of publication allows design owners seeking protection through registered Community designs to request that their registered design be published up to 30 months after the filing date.

Original designs that have become public domain before their owner had a chance to sell a single item

It's no secret that famous designers have their unique designs copied the moment pictures or videos from the catwalk hit the (social) media. What an awkward moment it must be for a prominent client of an unnamed luxury brand sporting the designer's latest style to bump into a less prominent client of an unnamed retail chain wearing the "same" style from a general retail chain – the latter style apparently having cost its owner ten or more times less. Inevitably, a client's motivation to buy more expensive and apparently not-so-unique styles is weakened, while the less prominent client assures himself that the logic of "why would I buy overpriced clothes if I can get the same style ten times cheaper from a retail chain?" is correct.

One could argue that the fashion industry did this to itself by adopting the somewhat unfortunate practice of publicly displaying next year's spring / summer collection in autumn of the previous year.

So besides not disclosing their designs to the whole world half a year before they appear in stores (meaning their own stores), what can creative fashion designers do to protect their designs from this kind of exploitation?

Design protection in the EU

Fashion styles such as designs of clothes, bags, shoes or hats may become protectable as registered or unregistered designs, depending on their level of uniqueness and novelty, and other criteria. At the EU level, Council Regulation (EC) No. 6/2002 of 12 December 2001, on Community Designs (the "Design Regulation") lays down the conditions under which a design may enjoy legal protection as a registered or unregistered design.

Unregistered designs may be a practicable solution for small businesses and designers – beginners for whom the fact that legal protection arises only upon the design being made available to the public may not be an issue. For obvious reasons, unregistered Community designs are not an option for fashion designers who want their designs to be secret and protected at the same time.

Registered Community designs – delayed publication

Under article 49 of the Design Regulation, a registered Community design shall be published in the Community Designs Bulletin that is open to public inspection, ie may be freely accessed by anyone. However, article 50 of the Design Regulation introduces a so-called deferment of publication. This allows the design applicant to request, when applying for the design, that the publication of the design be deferred after its registration for a period of 30 months from the filing date (or priority date). As a result, the design will remain secret. It will be registered, but neither its representation nor any related documentation will be made available to the public.

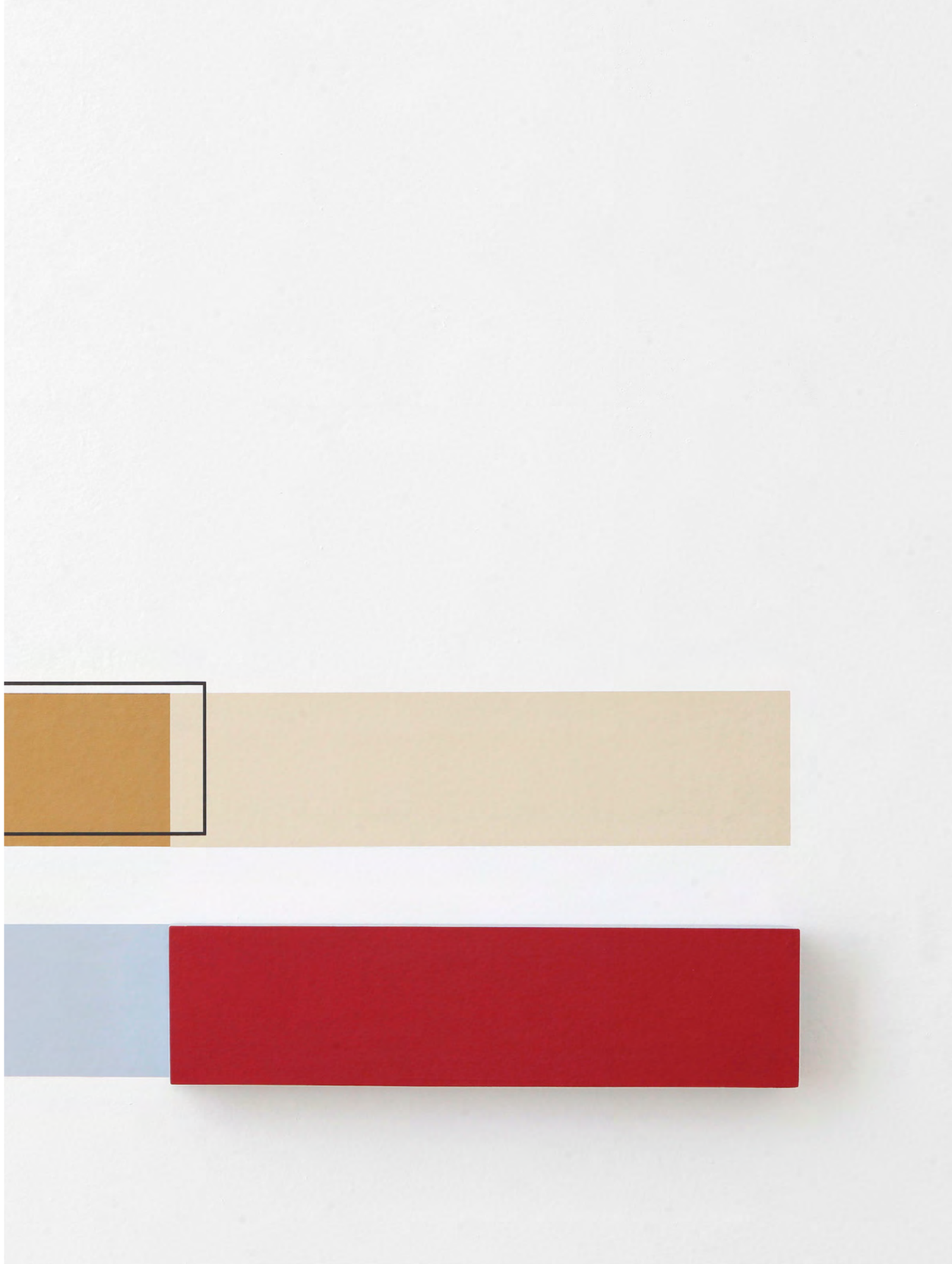
Solution for fashion designers?

How will this work in practice? Let's say a designer creates a set of unique, new dress designs that he perceives as his signature designs. The designer applies for a set of Community designs and requests deferred publication. By the time the dresses are shown on the catwalk, the designs are already protected by registered Community designs, but have remained secret and unknown to the public. The moment the designer spots that his signature designs have been copied and are sold by other retailers, the designer may take immediate action (typically applying for a preliminary injunction) to prevent further sale or marketing of the copied garments pursuant to article 19 of the Design Regulation, in conjunction with articles 9 and 10 of the Enforcement Directive (Directive 2004/48/EC of the European Parliament and Council of 29 April 2004 on the enforcement of intellectual property rights).

For designers who can afford to apply for a Community design protecting the most distinctive pieces of their current collection/s (and who can afford to pay the associated enforcement costs), deferred publication may seem like a partial solution. Partial in the sense that not all designs are eligible for design protection and that no designer can afford to obtain design protection for an entire collection several times a year (pre-collections, standard collections, limited editions, etc).

Conclusion

In the world of fast fashion, digital media and global mass production, designers and artists face increasing challenges to their creativity. Massive copying undermines the value of creative work and deprives artists of their livelihoods. Registration of a Community design with deferred publication offers certain recourse, although designers must be prepared for increased costs: the minimum fee for a single design registration with deferred publication is EUR 270, with another EUR 120 for subsequent publication. While large fashion houses can afford to invest in the legal protection of their designs (with these costs ultimately being passed on to consumers), for individual artists, the costs of registering a design may be prohibitive.



A "private sphere" for entrepreneurs – are you ready for the new Trade Secrets Directive?

Dominik Hofmarcher

While companies generally do not have a right of privacy (at least under Austrian law), the protection of trade secrets has a somewhat similar objective: to grant leeway for development, which others must respect.

Why is this important? The content of this article was a secret until I submitted it. Now it is protected by copyright law and therefore must not be copied without permission. This example illustrates a very common sequence: Idea > confidential realisation (trade secret) > publication / registration (Intellectual Property Right, "IPR", be it a copyright, trademark, design or patent). Or as the European Commission put it almost poetically: "Every IPR starts with a secret."

In fact, not only IPRs but of course all commercial activities start with an idea and thus a secret. Some might be trivial, but others are brilliant and valuable. And while certain ideas or concepts may later be protected by registered or unregistered IPRs (like this article), other information is kept secret because:

- no adequate IPR is available (eg to protect customer data, delivery conditions, etc);
- protection (eg by patents) is too expensive; or
- protection as a trade secret simply has advantages (eg if reverse engineering is not possible, an invention may be kept secret to avoid publication).

Against this background, the protection of trade secrets is a necessary supplement to the protection conferred by IPRs. Being aware of this important function, the EU has recognised that the protection in the Member States is inconsistent and often insufficient. Thus, with Directive (EU) 2016/943, a modern and for the first time EU-wide harmonised regime for the protection of trade secrets was established. Member States will have to transpose the directive into their national laws by 8 June 2018.

Are you ready for the new regime? While the Directive will undoubtedly strengthen the protection of trade secrets, it requires owners to take care of their assets. Trade secret protection may only be invoked if the information in question has been subject to reasonable steps taken by the person lawfully in control of the information to keep it secret.

> With Directive (EU) 2016/943, a modern and for the first time EU-wide harmonised regime for the protection of trade secrets was established. Member States will have to transpose the directive into their national laws by 8 June 2018.

You are therefore well advised to identify your valuable know-how and business information and to implement protection measures right now. Until the courts give sufficient guidance, an initial "toolbox" of technical, organisational and contractual measures may include:

- implementing a secrecy policy;
- appointing a person responsible for the secrecy policy;
- reviewing compliance with the secrecy policy;
- limiting the sharing of information only to the people who really need to know it (in-house staff and external contractors), while
  - knowing their identity;
  - informing them about the secrecy policy;
  - binding them by a (contractual) non-disclosure obligation;
- storing documentation separately and securely (both paper and digital data by using locks / passwords / encryption).

Take good care of your ideas and trade secrets!

How to surprise the market: The secret trademark application

Christian Schumacher | Gudrun Irsa-Klingspiegl

Plans to introduce a new product or service are often kept secret for a number of reasons. The later one's competitors become aware of an entirely new product or service, the longer one will enjoy the benefit of being the natural leader in that newly created market. In addition, famous companies in particular try to generate hype by creating an aura of mystery and focusing the public's attention on the big upcoming launch.

But it's not all just for show. Once a large company reveals a new brand, hijackers may rush to register internet domain names or trademarks, hoping to receive a ransom in return. This is particularly troublesome with internet domain names, which for technical reasons can only be delegated once.

If you don't get mynewbrand.com, internet users may not find your new product or service as quickly as you wish. And if a certain trademark is grabbed and registered in a trademark register before you can do it yourself, especially in less developed jurisdictions, you will have to make a disproportionate investment to convince the authorities that the trademark was registered in bad faith and should be banished from the register.

Therefore, it is good practice to secure trademark priority by applying – at least in one's home jurisdiction – for a new trademark that incorporates the new brand as early as possible in its development. According to the Paris Convention, further trademark applications internationally can then enjoy the same priority, if filed within six months. However, trademark applications appear rather quickly in the public trademark databases, so everybody can see that the company applied for a specific trademark for specific goods or services.

Can a trademark application be filed secretly?

For design registrations, publication can be deferred for a certain period of time so that the design and its owner will remain secret. The owner can thereby secure priority for its design registration without informing its competitors about the new design before the time is right. Trademark law does not foresee a secret trademark application in such a way. But there is a practical way for companies to preserve secrecy relating to new trademarks: They can procure trademark applications through a trustee – maybe even in a different country – who will then appear as the applicant (and once registered, as the owner) of the trademark in the public registries and databases instead of the real applicant. The same applies to internet domain names.

In order to allow the trademark owner to easily take over and manage the "secret" trademark portfolio, the following needs to be considered before filing the application:

List of goods and services: if the trademark is used for goods and services that only a few companies provide in a country, even application by unknown applicants will quickly raise the attention of competitors. In order to avoid this, the goods and services of interest can be "hidden" in a much broader specification that might divert the notice of third parties. After the brand is publicly revealed, the goods and services that are not required can be deleted to avoid unwanted collisions and too high maintenance costs.

Filing strategy: it is easier to manage the portfolio in the future if the application is filed in the home country of the trademark owner in case an International Registration shall be based on this filing. Therefore, it is recommended to file the first application in another country only if it can be assigned to the trademark owner before the end of the Paris Convention priority.

Trustees and the trustors are advised to engage in a formal agreement securing their obligations once the trusteeship shall be released and the trademark shall be assigned to the trustor. Such an agreement is also useful in the event of trouble, for example, if the trustee receives objections from a trademark office or if the holder of an earlier trademark sends a demand letter or even initiates an opposition or cancellation action against a trademark application or registration or similar action in respect of a domain name.

Once the product or service has been launched and the brand has been publicly revealed, all the registrations for the trustee need to be transferred to the trustor. For a multitude of trademarks in several jurisdictions and domain names in several registries, this can be quite a complex, expensive and time-consuming task, as various formalities must be complied with for each trademark office and each domain registry. But that is the price of secrecy.

Mariana Karepova
President of the Austrian Patent Office.

"We offer a good deal"

An interview by Guido Kucsko

Guido Kucsko, head Schoenherr ip team in conversation with Mariana Karepova, president of the Austrian Patent Office, about secrecy and the value of disclosure by patent application.

Q: A patent office is perhaps not the right place for keeping technological developments a secret, because it publishes inventions as patent specifications and thereby adds them to that which is state of the art. So what could motivate inventors and innovative enterprises to give up keeping new developments a secret?

A: First of all, I must tell you that I disagree: the patent office is perfect at keeping secrets. At least until publication, there is no better place for new ideas and company secrets. This guaranteed non-disclosure is supplemented by many other assets: the date of filing an application triggers a very productive period: you (the person registering an invention), will receive an expert opinion, enjoy advisory services and receive a search report. This means you can prove the date of birth of your innovation towards third parties. At some point, however, a decision must, of course, be made. Now coming back to your question "Why should people give up secrecy?" Well, I would say we offer a good deal. You are compensated for publication by a monopoly right for the exclusive use of your invention. Globally speaking, this seems to be a lucrative offer for hundreds of thousands of cases per year – in short "an offer you can‘t resist."

Patents create a monopoly and curtail competitors‘ opportunities. How do you justify such monopolies? Shouldn't any kind of knowledge, every innovation be jointly owned by all?

This is very simple, the justification is a failure of the market: research, development and innovation take time and are expensive and risky undertakings for all companies. Just imagine your development takes several years, costs a lot of money, and you cannot protect it afterwards. I think we would have far fewer great breakthroughs without industrial property protection. Companies need incentives to invest in research and development. Nobody can bear the associated risks alone, therefore the state intervenes with research support and the patent system. Companies need time to earn back the costs of their development work. This sounds like dry theory – but inventors deserve recognition. When filing a patent, they make their acquired knowledge available to everyone. In addition to the sole right of use, inventors should therefore also be recognised for a certain period of time.

An innovative idea is the basic foundation of every start-up. How do patent offices – in particular the Austrian Patent Office – contribute to promote innovation and patent applications?
Start-ups are very special clients. They have to do everything at once, under immense time pressure: talks with investors, searching for partners and distribution channels. Under such circumstances they often forget the essentials: to file an application for their idea, to secure it before telling "family, friends and fools" and to make it tempting for possible investors. Unfortunately start-ups often lose million-dollar ideas this way.

We have therefore created a special procedure for young enterprises to file patents quickly and at a moderate cost: the provisional patent application, which young inventors can deposit in the "safe" of the Patent Office, even without having everything formulated as required for a patent application. The "date of birth" is secured – an upgrade to a full patent application is possible at any time during the first year. This possibility is used proactively by many start-ups – meanwhile 7% of all patent applications are provisional.

Of course patents are not the only instrument. We have also created a fast procedure for logos and brands: Fast Track, the new online trademark application. We are really proud of this superfast procedure: 10 days from the online application to the registered logo. That is not all – we have many plans such as creating a customer management model where individual mentors should be available for universities, heavy users and young users.

Under which conditions would you recommend innovative enterprises to keep their innovations a secret?
As the President of the Patent Office I would never recommend such a thing, because it is bad for my business. But seriously, there are criteria which might be taken into account for a decision. These criteria are generally known: this would be a long period of use which by far exceeds the lifetime of a patent and the quick and simple way to exclude re-engineering. Such a strategy may be successful in some cases. For example, Coca Cola as well as KFC use secrecy as a strategy. The recipe of the famous soft drink and the spice blend of the fast-food giant are kept in the utmost secrecy. But the risk remains. It is certainly always advisable to combine secrecy with other intellectual property rights such as trademarks and designs.

All countries discuss cost-cutting programmes by reducing costs of public administration. What is the economic benefit of a patent system?
Austria is one of the countries with the highest expenditure for research and development. Statistics Austria estimates the total expenditure in 2017 to be about EUR 11.33 billion. This is a very high investment in R&D made by companies, research institutions and governmental funding agencies. If you want, we can see the patent system as investment to protect at least parts of this expenditure. Results from research and development must be sufficiently protected to lead to marketable results. Without protection these investments would be lost, also for the public sector.

We are now on the eve of the European Union Patent, possibly even including the UK, despite Brexit. Do you expect new economic incentives from the EU Patent?
If we are now on the eve, there is probably a long night coming – at least a longer night, as we expected, because there seems to be further delay. The advantages are obvious: the EU Patent will make simultaneous patent protection in several countries possible, will be less expensive and will promote internationalisation. But of course this development also brings new challenges. One thing is very clear: we will not only file many patents, but will also be confronted with hundreds of thousands of rights to exclude from all over the world, which will suddenly be effective here in Austria. There will be a lot of work for us – for your profession and for us as the Patent Office.

Thank you for the interview.

08 labour & employment

Labour Law Developments in Light of the Basic Data Protection Act

Big Brother is watching you: Developments in employment law


Stefan Kühteubl | Karin Köller

The pervasive use of e-mail and the internet in the workplace has given rise to increased security issues, including data theft or misuse. But it has also given employers new ways to monitor employees, which leads to some interesting questions.

What is the legal basis for monitoring measures in Austrian employment law?
(i) The Austrian Labour Relations Act (Arbeitsverfassungsgesetz – ArbVG);
(ii) the Austrian Labour Law Harmonisation Act (Arbeitsvertragsrechts-Anpassungsgesetz – AVRAG).

Which monitoring measures are lawful?
The legal framework governing employee monitoring in Austria is complex. Control measures include any practices useful for monitoring employees and all technical facilities that are objectively suitable to monitor employees. The monitoring of job performance in general is a necessary and permissible method for the employer to ensure that its own products and services are successful. It is unlawful to implement monitoring measures that are offensive to human dignity.

The concept of human dignity must be defined in reliance on the general right to protection of personality and the fundamental values protected by the legal system, based on a balanced weighting of the interests of the employees and the employer. It is also usually permissible to monitor attendance.

Does a works council need to be consulted?
Yes. Under Section 96 (1) no. 3 ArbVG,

the "implementation of control measures and technical systems for employee control" requires necessary participation if those measures (systems) affect human dignity. If no works council exists, these control measures can be adopted pursuant to Section 10 AVRAG with the consent of each and every employee.

> Lay down detailed rules for the use of e-mail and on whether private internet browsing is generally allowed or forbidden and to what extent.

Control measures include any practices useful for monitoring employees and all technical facilities objectively suitable for this purpose. Whether monitoring actually takes place or whether the employer subjectively intends to monitor its employees is irrelevant. In addition, only monitoring measures established on a lasting basis must be approved pursuant to Section 96 (1) no. 3 ArbVG. *Ad hoc* controls, eg in connection with a (potential) criminal offence, do not require employee participation.

Notably, not all monitoring measures established on a lasting basis require employee participation – only those which affect human dignity. Consequently, those monitoring measures which do not affect human dignity are ones with no co-determination. Monitoring measures which affect human dignity require co-determination; those offending human dignity are unlawful.

A shop agreement is required for video surveillance, because human dignity will be regularly affected, eg in case of permanent monitoring and recording of entrances and exits. The monitoring of changing rooms, toilets and the like violates human dignity and is completely prohibited. It is also forbidden to directly and permanently point a camera at an employee's workstation.

If monitoring measures which affect human dignity will be implemented without a shop agreement, the works council may file an injunction or obtain a preliminary injunction in court. If such an injunction is granted, the employer has to stop the monitoring measures immediately or the court may impose high penalties.

Is monitoring employee e-mails permitted?
A technical system to monitor work e-mails is permissible, but is a so-called "control measure" that requires a valid shop agreement between the works council and the employing company.

If no such agreement exists, the employer may not take the envisaged measures. Monitoring e-mails containing obviously private correspondence is prohibited (ie the e-mail header is marked "private"), if the employee is using his work e-mail account, even if works council or employee consent has been given. Systematic monitoring of personal e-mail accounts is not permissible under any circumstances.

Can the employer monitor external website access?
Most legal scholars believe that systematic monitoring of external website access is not permissible. It may be argued, however, that storing log files of accessed external websites is permissible, but might qualify as a control measure that requires the consent of the works council in the form of a valid shop agreement – or where no works council is established, the written consent of every employee. Nevertheless, monitoring external website access may be justified in certain individual cases by the legitimate interests of the employer or be permissible if private internet use is generally prohibited.

What is keylogger software?
Keylogger software records keystrokes and creates regular screenshots on a computer. If used by employers, keylogger software enables an employee's activities on a work computer to be monitored, including any use for private purposes. The German Supreme Court held that the hidden use of keylogger software violates employees' personality rights, and that findings obtained by such monitoring software cannot be used as evidence in court proceedings (BAG 2 AZR 681/16). The hidden use of such keylogger software to monitor employees is only permissible if the employer suspects that a certain employee has committed a crime or other serious breach of duty.

Any recommendations on how to deal with monitoring measures?
A lawyer's recommendation is simple: Lay down detailed rules for the use of e-mail and on whether private internet browsing is generally allowed or forbidden and to what extent. Conclude a detailed shop agreement with the works council, or if no works council is established, obtain the employee's consent to monitoring measures.

Employee consent to data processing

Barbara Jóźwik

Under Polish labour law, an employer may request the following data from an employee:

- first name (names) and surname
- parents' names
- date of birth
- place of residence (mailing address)
- education
- employment record

An employer can obtain the above data without the employee's consent.

Due to the narrow range of personal data that employers are allowed to process under the Labour Code, employers also try to obtain and process other personal data of employees with their consent. Employers indicate that such consent is one of the conditions permitting personal data processing on the basis of the Act on Personal Data Protection dated 29 August 1997.

However, this practice is being challenged by the Inspector General for the Protection of Personal Data as well as by the courts for the following reasons:

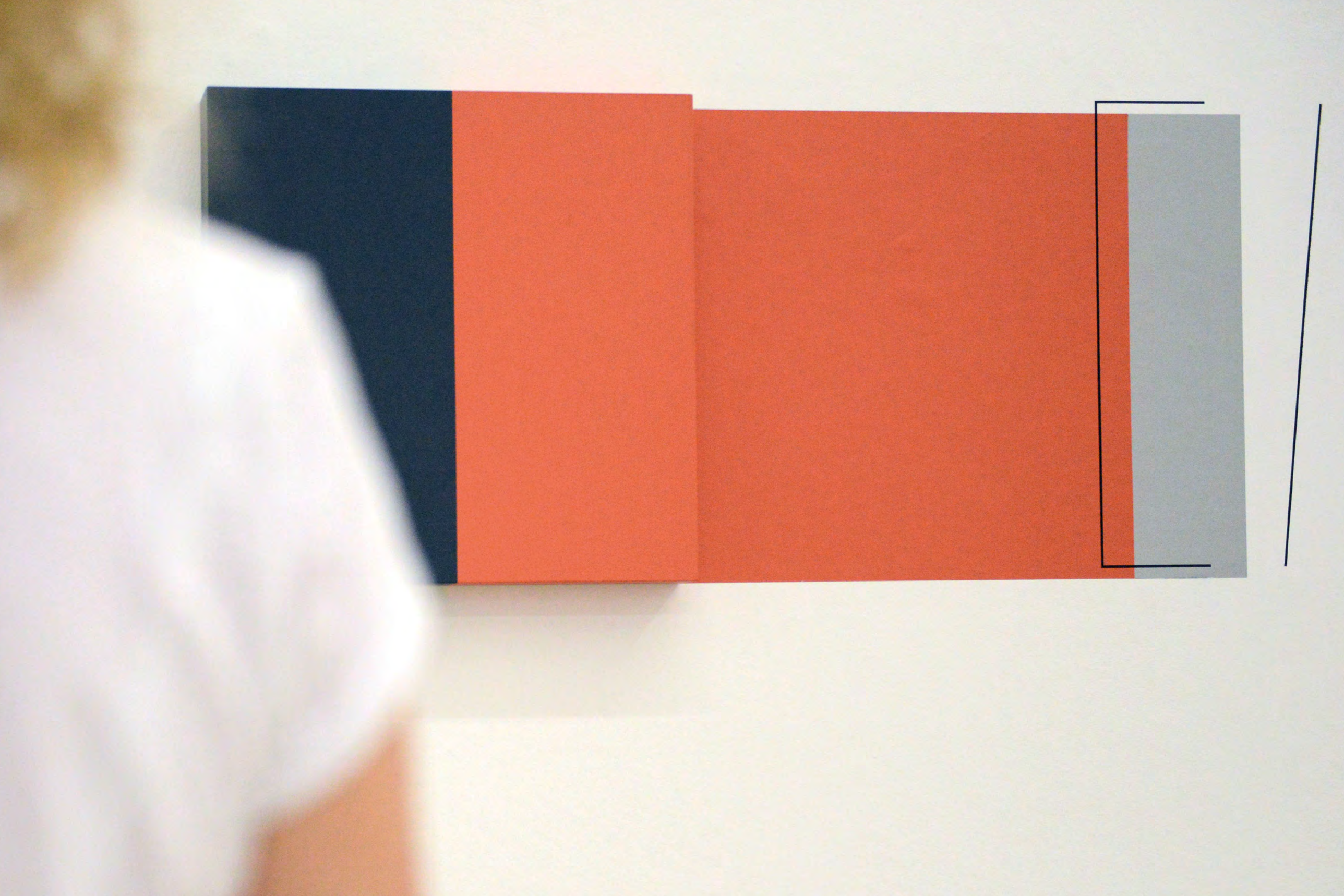
- consent, understood as one of the legal conditions permitting personal data processing, must be voluntary and freely given. The consent may be considered voluntary only where giving such consent or denying it has no impact on the employee's rights. Due to the imbalance in the relationship between an employer and an employee, the consent given by an employee cannot be considered voluntary;

- demanding from an employee additional data other than specified by the Labour Code or other legal acts is a circumvention of the Labour Code, which clearly states that the employee's (or job candidate's) personal data may be processed only on the basis of statutory provisions;

- only a legal provision may constitute a basis for collecting the personal data of an employee. If there is no such provision, an employer cannot request personal data from an employee, even if the employee gave their written consent.

The above opinion is very strict and does not allow employers to verify the job candidate or employee and to demand, for example, a criminal record statement when filling a position linked with financial liability, even with the employee's consent.

Under the General Data Protection Regulation 2016/679 ("GDPR"), which will enter into force on 25 May 2018, it is permitted to process employees' personal data with their voluntary consent. Therefore, it seems that under the GDPR it will not be possible to exclude the consent given by an employee as the basis for processing their personal data.



09 new technologies
Data Ownership

Claim for restitution of machine-generated data

Wolfgang Tichy | Günther Leissler | Michael Woller | Serap Aydin

New technologies in the courthouse:
How to restitute machine-generated data?
A fictional claim.

Claim for restitution of machine-generated data

Claimant:
XYZ Machine Learning GmbH

Represented by:
Schönherr Rechtsanwälte GmbH

Defendant:
123 Stolen Data OG

Due to:
disclosure, restitution, injunctive relief

Amount in dispute:
Euro 43.200 (§ 5 Z 14, 29 AHK)

CLAIM

The facts
The claimant is the creator of machine-generated data, which is in the defendant's power of control.

Machine-generated data is information which is collected or stored through measurement, observation, statistical surveys or other activities by a machine or a product. Such data can be personalised or non-personalised. When machine-generated data enables the identification of a natural person it is considered personalised data, therefore the data protection rules, in particular the general data protection regulation, apply.

The defendant is supplier of the claimant. It uses a software developed in conjunction with the claimant. The software automated collects and analyses motion profiles of vehicles which were placed on the market by the claimant. The data collection and analysis is completely anonymised and without reference to a person. This automated collected data is relevant and valuable for the improvement and development of the claimant's vehicles. Partially, the titles of the vehicles placed on the market are retained (Eigentumsvorbehalt) (especially leasing vehicles). For 3 months, the defendant refuses to give the data to the claimant, and makes use of the data itself. The claimant does not have access to the data because it is saved in memory, where only accessible by the defendant.

Evidence
Documents to be submitted; witnesses to be named.

Legal assessment
Until now there is no explicit provision, either on national legal level or on Union level, which regulates to whom the rights of machine-generated, non-personal data belongs and whether ownership of the data can exist.

According to the current legal situation, an owner of an object can proceed with his/her object at his/her own discretion and he/she can exclude others from any effect. That means that ownership confers on the one hand positively, a comprehensive right of use, and on the other hand, the owner can exclude others from utilisation (negative right of defence).[1] Since the data are indivisibly and logically connected with the vehicle, through which they generate analysis data, the claimant in any case derives (in so far as the vehicles are in favour of the claimant under the retention of title), the right of ownership over the vehicles that belong to the claimant through the retention of title and the right of ownership of the data as a negative right of defence.

Additionally, the claimant has copyright claims: The data, which are subjects of the proceedings are the result of a peculiar intellectual creation and therefore protected by copyright, as they are a direct result of the algorithm which is also created by the claimant as a joint author.[2] The creator of a database however has the right of preventing the extraction and/or the reuse of the whole or a substantial part of the contents of a database. The data generated by the machine on behalf of the claimant are, therefore, attributable to the claimant as a creator of the database.[3]

Business secrets[4] are protected against an unlawful appropriation as well as against an unlawful utilisation or disclosure. These machine-generated, non-personal data constitute an individualised analysis of the original driving behavior and are as such business secrets of the claimant and therefore protected against unlawful disclosure.[5]

Jurisdiction
The claim is among others based on the protection of business secrets. It is therefore a dispute over the infringement of industrial property rights. As a result, the commercial court of Vienna[6] is exclusively competent.

The claimant therefore desires the following judgement:[7]
1. The defendant is liable to make available all data collected through the software of the claimant concerning the vehicle placed on the market by the claimant within 14 days.[8]
2. The defendant is liable to release all data according to section 1. in a structured common and machine-readable format,[9] whereby the ascertainment of the data remains reserved until the successful announcement of the data according to the section 1 of the verdict.
3. The defendant is with immediate effect required to refrain from using the data under section 1. and /or essential parts of it, in particular of utilising the data for internal purposes, of transmitting or revealing the data to third parties.
4. The defendant is furthermore required to pay the claimant the legal costs according to § 19a RAO for the attention of the defendant´s representative within 14 days.

1 However, the condition is, that the data are objects in the meaning of the law. Objects are only material items and data by itself is not embodied, so there is no right of use established by property at the moment. According to the view of the European Commission, rights of the collected data can be attributed to either the producer of the machine or device, or to the economic operator, who operates and has paid for the machine or device. Furthermore, insurance companies, internet providers, and finally the State may have an interest in attaining the rights of the collected data. It remains open, to whom the rights of the collected data will belong and how they will be arranged. The justification of the capacity to sue (= the authority of the claimant to legally assert civil claims, which are entitled to him in his own name) seems to be challenging.

2 The defendant will oppose the fact that the machine-generated data sets lack originality in the sense of copyright, and thus preclude copyright protection.

3 The protection of databases and industrial property right designed as ancillary right basically grants the creator of the database only injunctive reliefs, removal claims and payment claims. A right of surrender of data is not expressly mentioned by the law.

4 Currently, there is a fundamental protection of business secrets via §§ 11 and 12 UWG as well as the general clause of § 1 UWG. This protection should be clarified and reinforced by the imminent implementation of the directive of protection of secrets (Geheimnisschutzrichtlinie).

5 The UWG also essentially provides injunctive relief and removal claims. A right of surrender of data is not expressly regulated in the UWG.

6 It seems unclear, if the rules of jurisdiction according to § 53 JN are applicable to the infringement of the business secrets. A transfer of the legal matter to the not obviously incompetent court of the defendant could be necessary.

7 To ensure the injunctive reliefs an application of an injunction (directed on the temporary omission for using the data) could be applied for. Additional a claim for surrender could be applied through an injunction.

8 In the Austrian civil procedure law, the principles of the certainty of the claim prevail. The claimant is supposed to concretise what it demands from the defendant. One exception to this rule is the "multi-stage claim" (Stufenklage). Thus, claims can be filed, even if the amount of the claim is not known. Therefore, the multistage claim could also work for the claim of surrender of data. In a first step, one can require the announcement of the data collected by the machine or the device and in the subsequent step the release of those data. It remains to be seen whether the courts will follow this approach.

9 If the right holder of the machine-generated, non-personal data has legal right of a special format of data, portability remains open. The analogous application of rules of the data-protection-basic regulation (Datenschutz-Grundverordnung) is conceivable in this case. In this regulation, the right of data portability is regulated. According to this the individual has a right to transfer his/her personal data from one responsible place to another in a structured, common and machine-readable format.

10 real estate & construction

My Home is My Castle

Do video cameras compromise privacy?

Natalia Wolfschwenger

In an increasingly digitalised word, privacy is playing an ever more important role in property law. Thanks to security cameras, drones and other new technologies, each of us may be recorded or photographed without our knowledge. The jurisprudence has therefore had to address the question of whether installing video cameras or photographing neighbours or tenants in a residential complex infringes on their privacy.

Trouble in the neighbourhood

It can be hard sometimes to get along with your neighbours in a residential complex or apartment building. There is a risk that other inhabitants will be recorded by, for example, installed video cameras. In a recent decision, the Austrian Supreme Court dealt with the question of whether landlords have the right to terminate lease agreements with tenants who have recorded or photographed others without their consent.

In this case, a tenant installed a video camera on his carport, which also recorded other inhabitants of the house passing by. The tenant also took photos of other tenants while they

were mowing the lawn or sunbathing. The Supreme Court concluded that this constituted a significant disturbance of peaceful co-existence and that the tenant was therefore guilty of seriously and continuously intervening in the inhabitants' personality rights. Harmonious co-habitation between the tenant and other inhabitants of the complex could no longer be expected. The landlord was therefore able to terminate the lease agreement for good cause due to the tenant's intolerable behaviour and the tenant had to move out.

Video cameras are commonly installed in housing and garage areas with the aim of protecting property. The established jurisprudence also allows the installation of video cameras as long as they are only in one's own living area and do not give neighbours the impression that they are being monitored, eg due to the position of the camera. The Supreme Court makes no distinction between real and mock video cameras, which are not recognisable as such. Thus, if a neighbour is subject to constant monitoring pressure, this shall be considered serious interference with his privacy. The neighbour therefore has the right to demand the removal of such cameras.

The use of drones remains a problematic grey area in the jurisprudence. Among the difficult questions requiring clarification are:

- who is controlling the drone?
- how do drones infringe privacy?

As there are no clear-cut answers, justified claims are not usually pursued. However, if a drone flies over a private property and the identity of the person controlling the drone is known, the owner of the property can defend himself against the infringement of his privacy by filing a trespassing claim under Sec 339 of the Austrian Civil Code. This is because, according to Sec 297 of the Austrian Civil Code, the vertical air space above a property is usually linked to the property itself.

Legal trespassing


Jana Cvirn Adamčić | Ksenija Šourek

Nobody's allowed on my property without my permission! Actually, that's not always true.

Most civilised societies regard the protection of one's property as a basic right (in certain jurisdictions as a constitutional right), and it is protected by law. However, the protection – which is at the same time a limitation for others – is not absolute. Here are five real-life examples of legal "trespassing" on property:

- **Misplaced things:** if your neighbour's dog wanders into your courtyard, your neighbour may access your property in order to retrieve his dog. You can prohibit the neighbour from accessing your property, but only if you immediately give him his dog. The same applies to other things the owner (or possessor) claims back from your property.
- **Necessary construction works on a neighbouring house:** if access and use of your property are needed for construction works on a neighbouring property and you deny access, the neighbour may sue you (and win). Nevertheless, you are entitled to compensation for the use of your property and the neighbour must remedy any damages caused due to such use.
- **Necessary passage:** if there is no alternative access to the neighbouring property other than over your property, the owner of the neighbouring property is entitled to use your property for such passage. Such use is limited to the necessary minimum and has to be formally established (servitude).
- **Placement, access and repair of utilities (eg sewerage pipeline):** if it is in the interests of the state, it can be done on your property without your consent.
- **Interventions by authorities (police, firefighters, etc):** in special situations (eg criminal acts, immediate danger), authorities may access your property without your approval.

There's no place like home until the neighbour interferes


Franziska Oczlon | Christoph Tittes

Turn the page to read more

My home is my castle. **Unfortunately, the Austrian Supreme Court ("OGH") doesn't think so. The Austrian Civil Code (ABGB) entitles property owners to prohibit all emissions that exceed the local norm and have a substantial effect on the customary use of their property.**

Here are some rulings that the OGH has made since 2011:

• **Smoking on the balcony** (2 Ob 1/16k)

Those who wish to smoke on the balcony of an apartment building must balance their interests with those of their non-smoking neighbours. As there was a lack of consensus of the neighbouring parties in this case, the OGH ruled that it is forbidden to smoke on the balcony during night hours (10:00 pm – 6:00 am) and during certain periods of the day (8:00 am – 10:00 am, 12:00 pm – 3:00 pm, 6:00 pm – 8:00 pm).

• **High cypresses shade neighbouring plot** (1 Ob 84/16h)

Owners of cypresses that completely shade a neighbour's plot after 3:00 pm are obligated to trim the cypresses.

• **Trees in a residential area (8 Ob 59/15g)**

An apartment owner claimed that his neighbour's trees prevented sunlight from reaching his property. The OGH stated that at the time the owner bought the apartment he could not have reasonably expected that the saplings in his neighbour's plot would grow uncontrolled to their current size. Therefore, if trees block daylight to an unacceptable degree, the neighbour must trim them.

• **Rock band rehearsal** (2 Ob 166/14x)

The owner of a cellar in an apartment building leased the cellar to rock bands. Although the apartment building is located in the city centre, the OGH stated that a typical neighbour would find prolonged rehearsals annoying. Therefore, the owner of the cellar is obliged to stop them.

• **Wildly rampant greenery on roof terrace** (8 Ob 78/13y)

If planting on the roof terrace is uncustomary for the site and attracts wild pigeons, neighbours are entitled to request that the owner of the roof terrace remove the plants.

• **Cat on neighbouring plot** (5 Ob 138/11x)

The owner of a plot has to accept that a neighbour's cat may enter and soil his plot, as there is no legal obligation to keep cats indoors and the tethering of cats is not allowed.

• **Chickens on a neighbouring plot** (10 Ob 52/11m)

The owner of a plot is obliged to fence off his plot if he releases his chickens every day from 2:00 pm until twilight and if his chickens enter neighbouring plots.

Do our smart devices have the right to remain silent?

Tamás Balogh

On 20 July 2017, a burglar sneaked into a family's flat in Hungary, grabbed whatever valuables he could find, and disappeared without a trace. At least that's what he thought. Unfortunately for the burglar, his crime was recorded by the family's baby monitor.

The family handed the video over to the police and the burglar was identified. In this case, it was clearly adequate for the police to use the footage in making an arrest. But what if the footage had been stored on an external server operated by a third party? Could law enforcement authorities request its disclosure even if it was unclear that evidence had been recorded?

Under the current data protection regulations, the answer generally would be yes. Law enforcement authorities would not only be entitled to request such information from the server operator, but also impose a fine for non-compliance.

But with the growing popularity of smart devices that collect and transmit information in our homes, the real question is whether there are clear boundaries for such data requests: Do our smart devices have the right to remain silent? Under the current data protection regulations, there is no clear answer. As it now stands, the law enforcement authorities are only obliged to describe the subject and purpose of their data requests, but generally do not have to satisfy any further requirements.

Although our private and family life, our home and our thoughts are protected by data protection regulations, they are not absolute rights. These rights may be restricted in accordance with the principle of proportionality, meaning they must be balanced against other rights and legitimate interests. Thus, in order to ensure that any restriction is proportionate, law enforcement authorities must at least evidence that there are no other options to obtain information for their investigation. Additionally, authorities shall also show the increased importance and necessity of their data requests.

Protecting the data collected by our smart devices, setting the virtual walls of our private homes remains one of the core tasks of the new Hungarian Act on Criminal Procedure that enters into force in July 2018. Despite that the principle of proportionality is already integrated into the new regulations, the detailed rules of data collection are still to be specified by separate legislative provisions that are expected to be adopted in the near future.

> “
> Although our private and family life, our home and our thoughts are protected by data protection regulations, they are not absolute rights.

An easy way to protect property rights in Poland



Agata Demuth | Jan Bagatela | Konrad Bisiorek

Claims resulting from the possession of property are the easiest way of protecting rights to use the property.

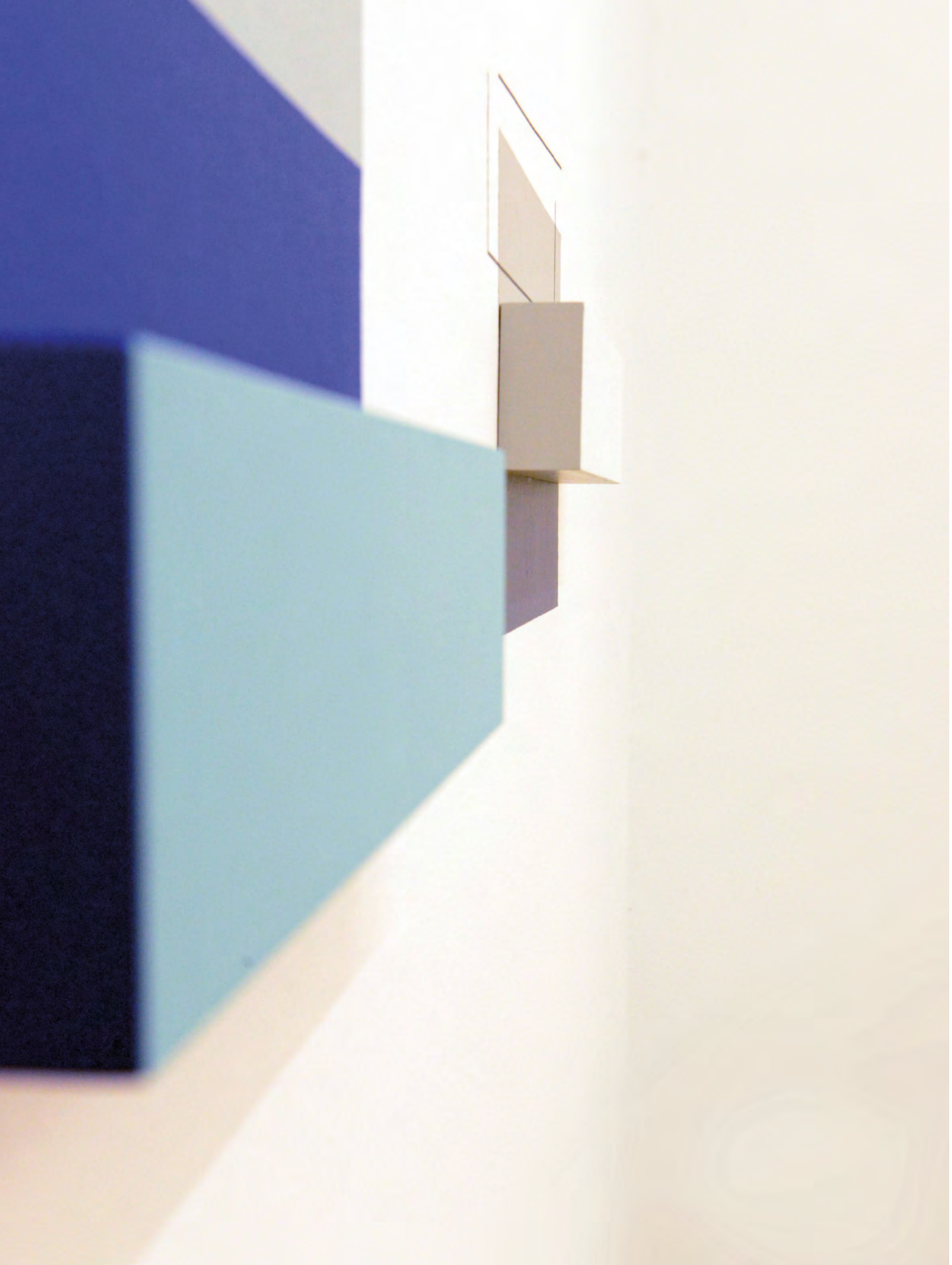
In line with a general principle of Polish law, possession cannot be wilfully infringed. Each property possessor such as an owner, tenant, usufructuary or even a possessor not having any legal title to the property can claim the restoration of possession. In the court proceedings the claimant must prove only the latest state of possession and its infringement. The court proceedings on possession protection are designed to be fast and effective, meaning that claims based on possession infringement are assessed relatively quickly.

The court is not entitled to verify any other conditions, in particular the possessor's legal title to the property or his good faith. Counteractions are not permitted, and hence claims can be successfully raised even against the property owner, who is not allowed to prove his rights to the property in such proceedings. If the owner wants to recover the property from the possessor, it has to start a separate action and prove his legal title. However, if the owner is simultaneously a possessor of the property and his possession was infringed, he can benefit from the possession-related claims against any third party.

A claim to restore possession expires if it is not made within one year of the breach. After this time, the possessor has to support his claim in court with a legal title to the property, such as ownership or tenancy, in order to restore possession.
It is worth mentioning that tenants enjoy basically the same level of protection of their right to use the premises as owners. This includes vindication claims if possession of the premises is assumed by a third party, and claims for cessation of other infringements of the tenant's right to use the premises (eg noise or other emissions).

Possession-based claims are often used in daily life, for instance:
- when the landlord blocks access to the tenant's premises due to any reason and without a court verdict, the tenant may request that such access be restored;
- when the landlord cuts off utilities (electricity, water, etc) to the premises, it can be treated as an infringement of possession and the tenant may request that the utilities be restored;
- when someone uses the neighbouring property to access its own property and the neighbour blocks such access, such access might be unblocked, at least temporarily; and
- when someone starts constructing a fence or a building on the neighbouring property, the construction can be stopped under protection of possession claims.

> “
> Article 344 § 1 sentence 1 of the Polish Civil Code: "A possessor can claim restoration to the previous state and cessation of infringements against a person who wilfully infringed possession, and against a person to whose benefit the infringement took place."



11 regulatory
Data Privacy

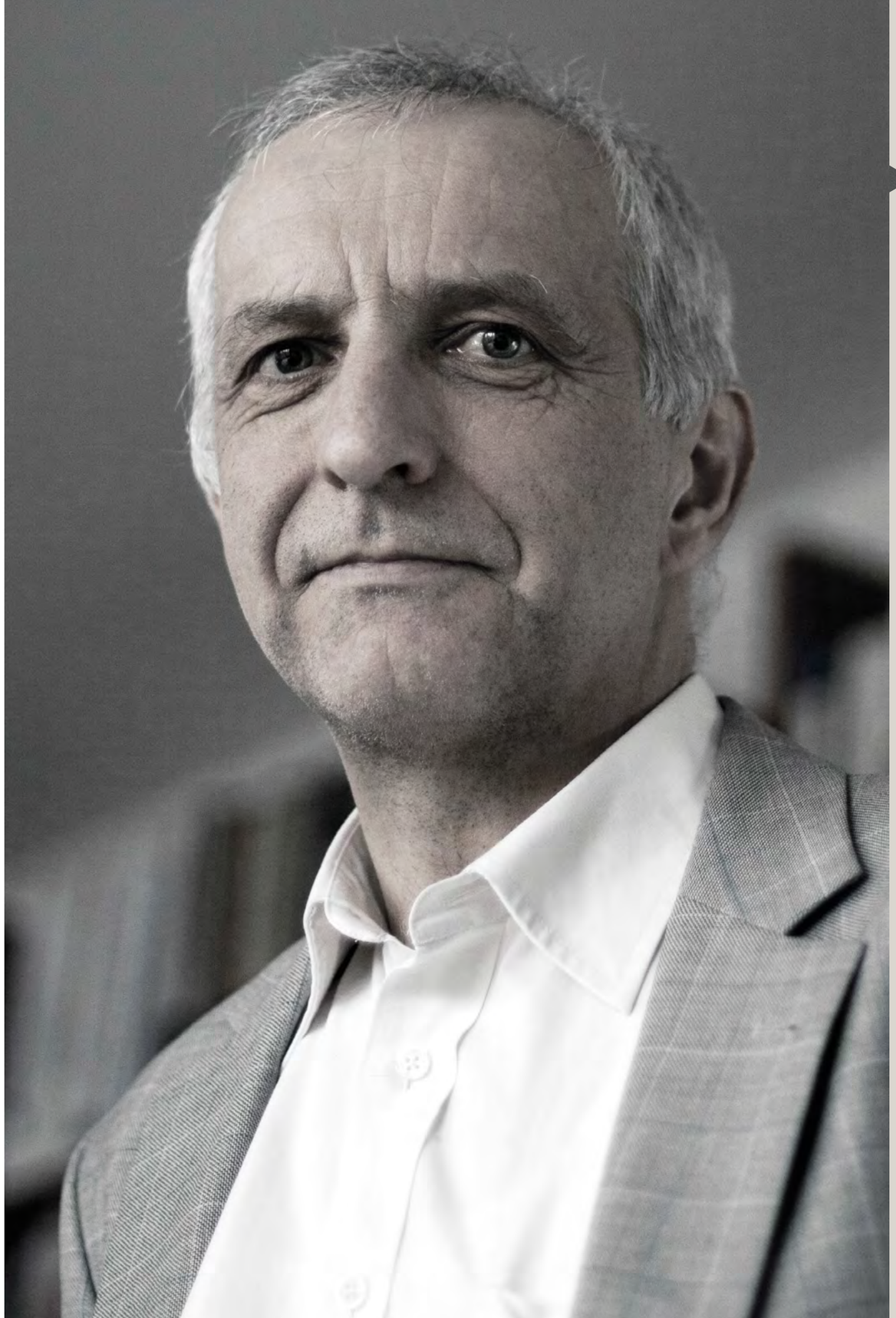
Data Protection on the move: A glimpse into the future!

Günther Leissler

In May last year a German lower federal court ruled that the use of WhatsApp is not legitimate without having obtained consent from those individuals whose contact data is uploaded to a WhatsApp messenger account (AG Bad Hersfeld, 15.05.2017 – F 120/17). The court considered the fact that WhatsApp automatically uploads the phone numbers of all contacts in a smartphone's address book. In its standard terms and conditions WhatsApp declares the following:

*"**Address Book.** You provide us the phone numbers of WhatsApp users and other contacts in your mobile phone address book on a regular basis. You confirm you are authorised to provide us such numbers to allow us to provide our Services."*

In the court's opinion, this automated upload infringes other user's rights of self-determination if done without their consent. No less important, the court even ruled out implied consent of those users were already subscribed to WhatsApp and, as such, should be aware of this automated data upload mechanism. In the ruling the court asked a mother to produce the missing consent of those individuals that had been uploaded by her son to his WhatsApp messenger account.



Thilo Weichert's take

Since this was the first case where a court not only scrutinised the legitimacy of cloud-based communications services, but also put the spotlight on the user's responsibilities when using such services, we asked Mr Thilo Weichert for his expert opinion.

Mr Weichert was the Federal State Commissioner for Data Protection and Freedom of Information in Schleswig-Holstein from 2004 to 2015. Besides other functions, he now works for the "Netzwerk Datenschutzexpertise". Mr Weichert is probably best known for his endeavours to ensure Facebook's data protection compliance over the past years.

An interview by Günther Leissler

Q: Mr Weichert, the District Court of Bad Hersfeld has passed two resolutions originally dealing with custody proceedings that ended up being a hotly discussed topic in the field of data protection. At the centre of attention is the messaging service WhatsApp.

In both cases, the court instructed mothers to produce the data protection declarations of consent of the entities who were uploaded on WhatsApp by their underage children. Do you think this marks a paradigm shift – a turn away from the user's status as a mere protection element in the world of social networks towards legal self-responsibility?

A: The decision does not mark a paradigm shift; it only describes the generally existing liability under civil law, data protection law and legal custody. To quote a famous German saying: "No plaintiff, no judge". This is a unique decision, as it is uncommon for a breach of privacy caused by an app to be taken to court.

Ever since I was a child, construction sites have had signs saying that parents are liable for their children.
Children are only to be held accountable for their actions in a limited way. This particularly applies for online activities. Who else but the parents should take responsibility in this case?

Mr Thilo Weichert (left) was the Federal State Commissioner for Data Protection and Freedom of Information in Schleswig-Holstein from 2004 to 2015. Besides other functions, he now works for the "Netzwerk Datenschutzexpertise."

The district court treated the question of the privilege of data protection in private data usage with wariness. In summary, it categorised the unauthorised uploading of telephone contacts as a private act, which failed to comply not primarily with the data protection law, but rather with the German tele-media act.

In your opinion, how big is the risk for companies that allow their employees to use their own mobile devices for both business and private purposes? This could lead to an upload of business data through their personal WhatsApp account. Could the company be held liable for a "bring your own device" policy?
Employers who allow staff to use their private smartphone for business purposes are even less savvy than the boy's mother. Business data is transferred onto the private device and therefore cannot be effectively controlled by the employer. The private device is, in principle, not subject to its direction rights. This requires a high level of trust in the employees. In any case, private and business matters on smartphones or tablets should be clearly separated from each other. If data is mixed, the employer is also partially responsible for the resulting data protection violations.

> In any case, private and business matters on smartphones or tablets should be clearly separated from each other. If data is mixed, the employer is also partially responsible for the resulting data protection violations.

WhatsApp users implicitly acknowledge and approve that their contact details are uploaded to WhatsApp through other users. However, the district court surprisingly emphasises that there is no such "implied consent", because the underlying technical processes are too complicated for the individual user. Does this pose a general risk for the agreement model in other apps and programs with a high degree of networking, even with explicit declarations of consent?
The argumentation of the district court is perfectly fine, as there is no such thing as legal valid implied consent. The requirements of consent are becoming even stricter with the General Data Protection Regulation, which comes into effect in May 2018. This has occurred through the instruments of "prohibition of linking" (Koppelungsverbot) and "privacy by default". One problem is that service providers still base their processing on largely inadmissible consents. Another is services with so-called layered design (graded), which is situation-related and with scarce information handling consent.

The court decisions we have been discussing are all in Germany, but the underlying legal ideas have their roots in general and European data protection principles. Do you think that the decisions of the magistrate's court are a flash in the pan?

Should we also expect court rulings in other Member States that prioritise self-responsibility of users?
Case law will certainly increase in this area with the entry into force of the General Data Protection Regulation, since additional possibilities for legal protection are created.

In addition, since the beginning of 2016, there have been improved opportunities for collective actions in Germany in the interests of consumers in the area of data protection.

In the past, we frequently saw decisions where the judges apparently did not understand the technical, economic and social conditions. Hopefully this will improve in the future, too.

Lastly, we have a stable jurisdiction with awareness of data protection on the part of the German Federal Constitutional Court and the European Court of Justice.

And yet, to take the metaphor further, there are plenty of indications that in the area of data protection the "flash in the pan" may become a judicial blaze.

Thank you for the interview.

Our take:

When taking a look at the German court's reasoning, it appears that individuals can be held liable when using WhatsApp and companies could be held liable when allowing their employees the use of WhatsApp on their business devices.

This is even more precarious with the GDPR on the horizon. So, where do companies stand with their preparations for the GDPR, and could the considerations of the German court have a legal impact on other jurisdictions as well?

A selected country overview from the authors below shows the following:


Günther Leissler
Austria


Stefana Tsekova
Bulgaria



Nina Petkovska | Magdalena Petreska
Macedonia



Pawel Halwa | Natalia Tokarz
Poland




Marija Zdravkovic | Pavle Tasić
Serbia & Montenegro

Ana Vukčević
Montenegro


Michal Lučivjanský
Slovakia

On their path towards the GDPR, what challenges do companies typically face to achieve compliance?

Austria:
In our view, different companies have different roads to the GDPR. Some already have fairly good knowledge of data protection and related requirements, while others are total novices in this area. However, most companies typically struggle to determine their data processing landscape, in particular as regards international data transfers. Yet, such an assessment is an indispensable requirement in order to properly determine compliance gaps that need to be filled before the GDPR comes into force. Other fields where action is required typically do not properly define (or are even missing) data processing agreements, consent declarations and, of course, implementation of the new concepts of the GDPR, such as records of processing activities, the concepts of privacy by design / default or of data portability.

Bulgaria:
Most companies are well aware of the upcoming changes, but only a few have already taken active measures towards compliance. A significant portion of companies are in the very early stages of launching their GDPR compliance programmes. The main challenge is to implement the GDPR requirements for the personal data that they are already processing and that is historically collected and stored in various places and systems in both hard and soft copies. The localisation of such historically collected personal data seems to be a common hurdle, but an important one to overcome in order to apply the new rules and principles.

Poland:
The changes brought about by the GDPR are commonly regarded as a positive development toward greater coherence between the broad range of national rules. Nevertheless, satisfying the demands of the new regulation requires practitioners, ie entrepreneurs and companies to specifically observe its demands on clarity and transparency of data processing. As recent studies show, even though almost 90% of Polish company managers have come into contact with the GDPR provisions, more than three quarters of them are not aware of the severity of the financial penalties for non-compliance. What's more, companies are having trouble identifying the entities within their business structures responsible for compliance with new regulations. A company's ability to incorporate the GDPR is also broadly assessed in respect of its consistency in introducing up-to-date technologies and the ensuing burden of additional costs. Only one-third of enterprises invested in advanced tools to manage data security and prevent leaks of sensitive information.
Polish companies could rely more on lawyers in order to familiarise the business teams with the new rules. On the other hand, compliance will not be achieved without closer and multidimensional cooperation between lawyers and IT professionals.

Montenegro:
Since the GDPR applies not only to organisations located within the EU but in certain cases also to companies outside the EU, the main issue for local companies will be to precisely determine if and when the GDPR applies to them, and if so, which obligations in particular.

Implementing internal policies, processes and controls with the aim of mitigating risks related to privacy and confidentiality will be another issue for local companies on their path to the GDPR.

Further harmonisation of the regulatory framework in Montenegro with the GDPR is also expected in the near future.

Serbia:
While in some cases the GDPR constitutes obligations for controllers and processors not established in the EU, we assume that Serbian companies operating in the EU will mostly face issues with respect to the applicability of the GDPR. As Serbian companies generally lack awareness of data protection, especially the obligations arising therefrom, it is realistic to expect a lot of issues in terms of compliance with the GDPR. In this regard, the obligation to appoint a representative in the EU under certain conditions (or the question of liability in the event of non-compliance with GDPR), seems to be the kind of issue that will raise doubts amongst Serbian legal entities. On the other side, the existing legal framework in Serbia does not provide a solid enough basis for efficient data protection in practice, and is not compliant with the rules of the GDPR. However, a new Act on Data Protection is expected to be adopted in early 2018, and will be harmonised with the GDPR, therefore decreasing the amount of uncertainty in practice.

Macedonia:
Most companies in Macedonia seem fairly well informed and responsive as regards data protection and their obligations under the data protection laws. The Directorate for Personal Data Protection has put in place many encouraging features to support greater awareness and to ensure that officers know about the changes in data protection regulations. This is done through regular training and workshops for data protection officers, but also through regular compliance controls of designated officers in companies. As Macedonian data protection law is largely in line with EU law, there are not many bridges which need to be crossed at this stage before the coming into force of the GDPR.

The GDPR is about regulation, but the recent court ruling in Germany shows a trend towards increased self-responsibility. Do you think your domestic courts might follow this path and establish case law focusing on the self-responsibility of the user?

Austria:
Austrian case law has long been dominated by a focus on protection, in particular with respect to B2C relationships. The Austrian Supreme Court imposed very rigid formal requirements on individual consent when this consent should form a valid legal basis for the processing of that individual's data. In a nutshell, we would not expect the Austrian courts to increase the self-responsibility level of users / data subjects in the near future. In fact, we would not be surprised if in light of the accountability standards of the GDPR, the Austrian courts might even increase the compliance standards on data controllers (ie the companies processing personal data). In our opinion, however, a very significant point of the German court ruling is the fact that the court has denied the implied consent of other WhatsApp users to their data being uploaded, since the court has concluded that WhatsApp users do not understand the messaging app's T&Cs, which prevents the court from assuming implied consent. This rigid interpretation on the validity of implied consent might easily be adapted by the Austrian courts, since it ultimately strengthens the data subjects' protection. Companies should thus be very careful when relying on implied consent to process personal data.

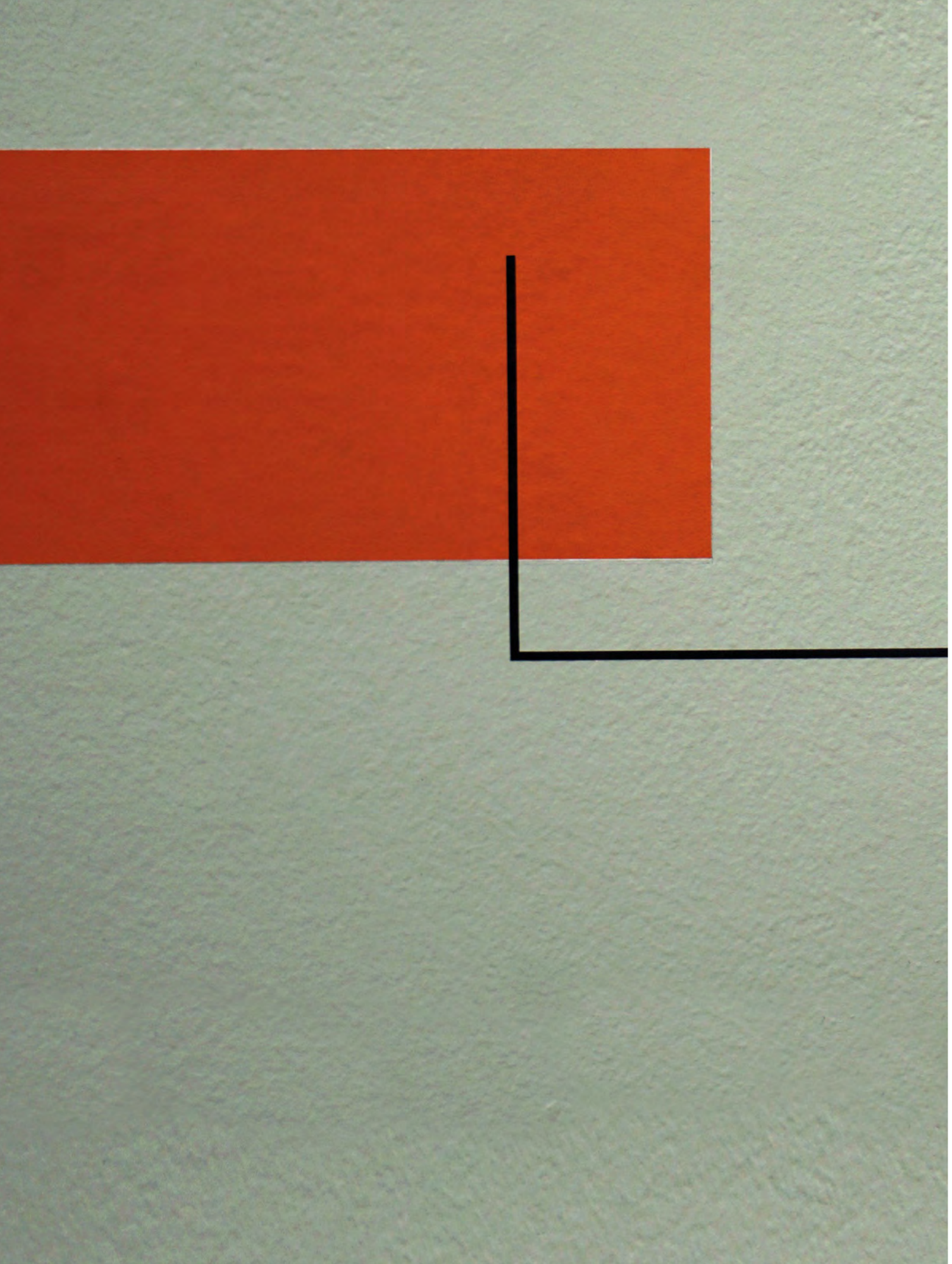
Bulgaria:
Bulgarian case law is poor on privacy disputes. So far the regulator and the court have interpreted the law very strictly and we do not expect the Bulgarian courts to increase the self-responsibility level of users in the near future. The main focus is on the business and not on individuals when processing personal data in the course of individuals' personal or household activity.

Poland:
The Polish courts approach the regulation of individual consent in quite a stringent manner. It is commonly assumed that such consent should be explicitly expressed. Moreover, the Supreme Administrative Court stated that the consent cannot be abstract, but should refer to the specific facts, including only the specific data and the precise manner and purpose of their processing. Separate consent to data transfer to third parties must be required, and the user must be granted optionality whenever giving consent to data processing. What appears more significant in light of the recent German ruling is that these restrictive conditions for data processing so far have been addressed exclusively to data controllers. Even though the German decision will not have a direct impact on the Polish system, the strict approach of Polish courts and other authorities is expected to continue following the entry into force of the GDPR. Since the GDPR rules are binding on the entities which effectively process data, the stricter responsibility will be attributed to the employees charged with these duties or, more likely, to the companies' management boards.

Montenegro:
Given the extremely modest existing case law on the subject, it is hard to predict whether domestic courts will establish case law that puts the focus on the self-responsibility of the user. The fact that court practice in Montenegro is not uniform makes it even more unpredictable. However, companies should take all necessary measures to implement adequate data protection and risk management processes, and view the practice of the European courts as a sign of possible further developments in the practice of the local courts.

Serbia:
Considering the lack of Serbian court practice in the field of data protection, it is difficult to anticipate trends in its further development. However, as regards implied consent, it should be stressed that the current Serbian Data Protection Act does not regulate and allow implied consent; it rather asks for express consent (eg in writing).
Implied consent shall be introduced by the forthcoming New Data Protection Act. Given that this new Act was prepared based on the provisions of the GDPR, it can be expected that once it is adopted, court practice will also shift towards the practices of the European courts.

Macedonia:
Macedonian data protection law leans heavily on the idea of consent, and companies are increasingly using explicit consent wherever data may be processed. This is deliberately aimed at avoiding the question of implied consent in the WhatsApp case. Taking into account the current Macedonian data protection law and reforms that are now underway, we do not expect much room to be left for self-responsibility. In addition, the Directorate for Personal Data Protection maintains regular controls of companies and their compliance with the law on data protection (on a regular, occasional and monitoring basis), and processors are heavily fined for non-compliance with data protection laws. For these reasons, we expect that Macedonian courts will most likely gravitate towards a more regulatory approach as per the GDPR.



12 tax

Tax Secrecy vs Exchange of Tax Information

Glossary


Mario Perl | Emilia Lhotka

BEPS (OECD):
Base Erosion and Profit Shifting (BEPS) refers to tax planning strategies used by multinational companies that exploit mismatches in tax rules to artificially shift profits to low or no-tax locations with little or no economic activity.

OECD Action Plan:
The 15 Actions proposed by the OECD should tackle BEPS. The Action Plan contains measures to increase tax transparency via taxpayer disclosure and tax authorities' exchange of information obligations.

Country-by-Country Reporting:
As part of the OECD Action Plan, it forces international groups to disclose their economic activities and respective revenues together with taxes paid for each country separately. This should avoid Transfer Pricing mismatches and result in fairer taxation. The EU implemented this reporting requirement in its Directive for administrative cooperation in the field of taxation.

Transfer Pricing:
Transfer pricing refers to the rules and methods to price transactions between related enterprises at arm's length, thereby taxing the entities on their actual and not their artificial income. This is especially relevant in cross-border situations in order to avoid BEPS.

Exchange of Information:
Cooperation between tax authorities of different countries is important to tackle tax evasion (mutual administrative assistance in tax matters). Exchange of information is one tool in order to discourage taxpayers from hiding their income abroad. Information may be exchanged spontaneously, upon request or automatically.

Automatic Exchange of Information:
Automatic exchange of information means that tax authorities have to collect certain information about taxpayers regularly and exchange such information with tax authorities in other countries. Within the EU, information is automatically exchanged on the following matters: directors' fees, pension and employment income, ownership and income from real estate, ownership of and income from assets on financial accounts, advance cross-border rulings, advance pricing arrangements and country-by-country reporting.

Tax Secrecy:
Tax secrecy prohibits tax authorities from sharing non-public information disclosed by the taxpayer in tax proceedings with any third parties. It facilitates the disclosure of information by taxpayers due to the confidentiality under tax secrecy.

Bank Account Register:
This is a centralised register for all bank accounts and deposits (Kontenregister) within Austria. It provides access to information about existing bank accounts and deposits to criminal prosecutors, financial criminal authorities and tax authorities.

Beneficial Ownership Register:
In the EU, Member States are obligated to register data concerning beneficial ownership of legal entities in a centralised database. The main purpose is to combat money laundering and terrorism funding more efficiently. Access is also provided for criminal prosecutors, financial criminal authorities and tax authorities.

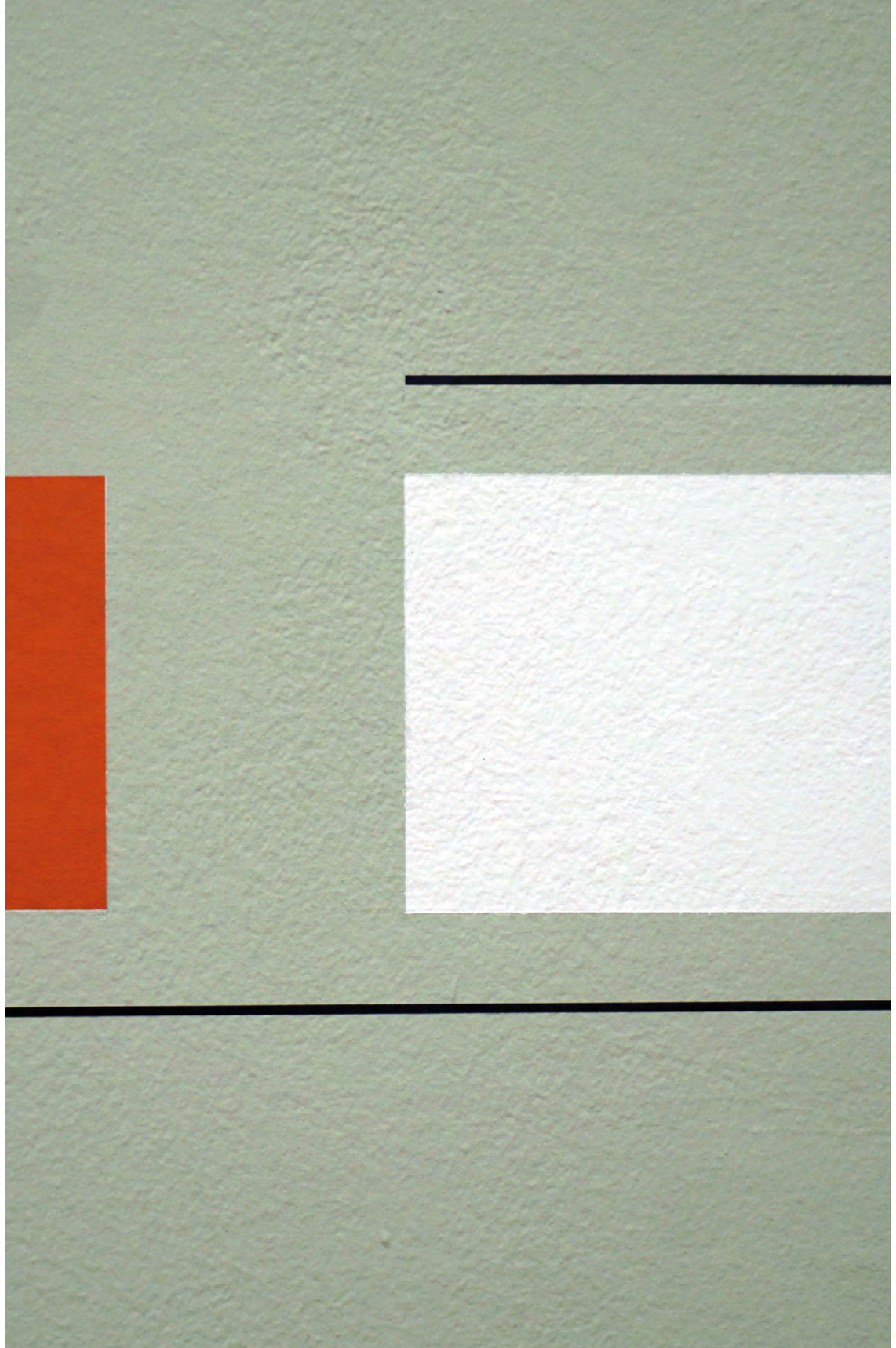
Access by tax authorities to new beneficial ownership register

Emilia Lhotka

Pursuant to a new EU directive, a beneficial ownership register has been adopted in Austria (see *Mandatory registration of beneficial owners Introduced for all Czech entities*, page 41). Based on the proposed draft of the Austrian Beneficial Owner Register Act, implementing the new EU Directive and Art 1 of the EU Directive 2016/2258 regarding access for tax authorities to such a register, access in tax matters to the register is provided to:

- criminal prosecutors and criminal courts in criminal tax cases;
- criminal tax authorities and tax courts in administrative criminal tax cases; and
- tax authorities and tax courts for tax matters, but only if this seems appropriate and proportionate in the respective case.

Non-compliance with the obligations to report relevant information to the Austrian register authority is subject to criminal tax prosecution according to the Austrian Fiscal Criminal Act (FinStrG).



Access for tax authorities to Austrian bank account information

Mario Perl | Emilia Lhotka

What is a bank account registry?
It is a centralised registry for all bank accounts and deposits (Kontenregister) in Austria, introduced in 2015 and operated by the Austrian Ministry of Finance.

What is the purpose of the registry and who has access?
The purpose is to provide information about existing bank accounts and deposits to criminal prosecutors, financial criminal authorities and tax authorities. Tax authorities generally have access only for the purpose of levying taxes if it is appropriate and proportionate. Access to income tax and VAT is restricted to cases where misinformation is suspected.

What does the registry contain?
(i) The accountholder's name, address, place of residence, and date of birth (in the case of individuals);
(ii) the account or deposit number;
(iii) the account or deposit opening / closure dates;
(iv) the name of the credit institution or the depositary; and
(v) information about trustors, beneficial owners and persons with authority over the account or deposit.
The account registry does not contain information about account movements and underlying transactions, and the account or deposit balance (sensitive information).

May tax authorities request sensitive information from credit institutions?
Tax authorities may also request sensitive information in qualified circumstances if (i) there are reasonable doubts regarding the correctness of information provided by the taxpayer, (ii) the requested information is expected to alleviate such doubts, and (iii) the request is proportional. A request regarding income tax and VAT is only possible after a formal request for clarification with a taxpayer's opportunity to comment.

What effect do bank secrecy rules have on access to the registry?
Tax authorities have access to the bank account registry and to sensitive information related to bank accounts due to an exemption from the Austrian bank secrecy rules.

How is privacy protected?
Every request for personal data by the authorities must be recorded. Every affected person has the right to information and every request has to be reported to the respective taxpayer. Access to sensitive information is only granted based on a decision by the Federal Tax Court, which may be appealed to a senate at the Federal Tax Court. An Officer for Legal Protection is responsible for safeguarding compliance with the legal procedure.

Privacy in the international exchange of tax information

Mario Perl

Directive 2011/16/EU (Administrative Cooperation in the Field of Taxation) established procedures for better cooperation between tax administrations in the European Union as regards information exchange, participation in administrative enquiries, simultaneous control, and notifications of tax decisions (the "Directive"). The Multilateral Convention on Mutual Administrative Assistance in Tax Matters of the OECD provides similar tools for states at an international level currently applicable in 112 jurisdictions (the "Convention"). Both legal instruments provide the obligation to exchange information between two or more states in tax matters. The following questions deal with privacy matters in relation to such international exchange of information.

Does bank secrecy or other confidential information prevent the exchange of information?
Under the Directive and the Convention, states may refuse to provide information that it is confidential towards the tax authorities or that may not be obtained based on the law or administrative practice. Information that would disclose any trade, business, industrial, commercial or professional secret or trade process or information contrary to the public policy (Art 17 (2) to (4) of the Directive, Art 21 (2) of the Convention) does not have to be provided. On the other hand, no state may decline to provide information solely because it is held by a bank, other financial institution (bank secrecy), nominee or person acting in an agency or fiduciary capacity (fiduciary secrecy), or because it relates to ownership interests in a person (ownership information) (Art 18 (2) of the Directive, Art 21 (4) of the Convention).

Is exchanged information still subject to national tax secrecy?
Information provided by one state due to the exchange of information shall be covered by the obligation of official secrecy and enjoy the protection extended to similar information under the law of the state receiving the information. Such information shall be disclosed only to persons or authorities concerned with the assessment, collection, enforcement or prosecution of tax in relation to the taxes of the receiving state for which information may be exchanged (Art 16 (1) of the Directive, Art 21 (1) of the Convention).

Information may only be used for other purposes if authorised by the authority that provides the information and only insofar as such information can be used under the law of the receiving state (Art 16 (2) of the Directive, Art 22 (4) of the Convention).

How is personal data protected?
Under the Convention, any information obtained by a state is treated as a secret and protected to the extent needed to ensure the necessary level of protection of personal data, in accordance with the safeguards which may be specified by the state providing the information as required under its domestic law (Art 22 (1) of the Convention).

The Directive contains a special provision regarding data protection (Art 25), and thereby refers to Directive 95/46/EC on data protection (after 24 May 2018 replaced by Regulation (EU) 2016/679). Certain provisions are declared not applicable for the correct application of the exchange of information to the extent required in order to safeguard interests in taxation matters (Art 13 (1) (e) of Directive 95/46/EC; Art 23 (1) (e) of Regulation (EU) 2016/679). Financial institutions that report data and tax authorities shall be considered data controllers for the purposes of Directive 95/46/EC (Regulation (EU) 2016/679). Financial institutions must inform affected individuals sufficiently in advance that personal data will be reported to authorities so that these individuals may exercise their data protection rights.

> The Directive and the Convention aim at a proper balance between the need for exchange of information and the need to provide safeguards for the rights of taxpayers and the states.

Romania: Disclosure of financial information of multinationals based on EU Country-by-Country Reporting implemented in Romanian law

Theodor Artenie | Anamaria Tocaci

Q: Has Romania implemented EU Directive 881/2016 on the mandatory automatic exchange of information on taxation?
A: Yes. Romania recently implemented the EU Directive in its tax legislation.

Who has these reporting obligations?
Ultimate Parent Entities which are part of groups of multinational entities having their tax residency in Romania or other reporting entities that meet the conditions provided in the law are required to submit an annual Country-by-Country Report, if their consolidated income is higher than EUR 750 million in the year prior to the reporting tax year.

What does the report contain?
The report should contain financial information such as: the aggregate revenues, profit / loss before tax, profit tax paid, declared capital, undistributed profit, number of employees and fixed assets. Also, the Country-by-Country Report must include information on each entity of the group regarding its tax residence and its main line of business. However, no actual format of the report has been provided so far.

When will the new reporting rules be applied in Romania?
The first reporting tax year is 2016, if the reporting entity is the Ultimate Parent Entity. If another group company (a constituent entity) is assigned / required to make a report, the first tax year to which the Country-by-Country Report should refer to is 2017.

What is the deadline for preparing the Country-by-Country Report?
The Country-by-Country Report should be submitted within 12 months from the last day of the group's reporting fiscal year.

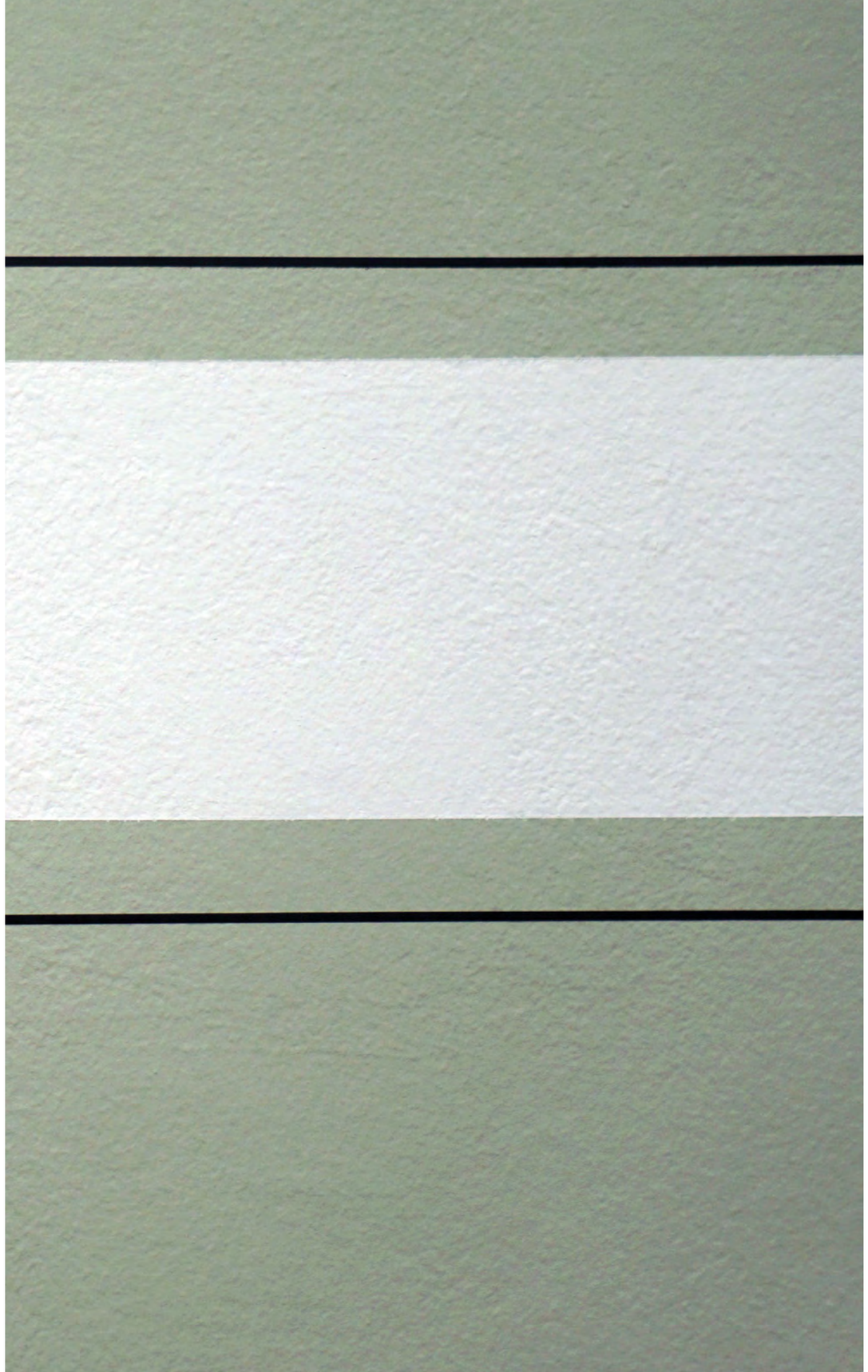
How will this help?
The Romanian tax authorities will automatically transmit the report to other Member States in which the group entities are tax resident or in which they have tax liabilities for carrying over business activities via a permanent establishment. Romania will also receive reports from other countries. In this way, the tax authorities will be able to combat aggressive tax planning (eg double deductions, double non-taxation).

How will this impact Romanian companies?
We expect that this reporting obligation will not impact many Romanian companies, given that Romania is not a preferred holding destination and given the large turnover threshold of EUR 750 million.

Comparison of tax secrecy in Austria and Romania

Mario Perl | Theodor Artenie | Anamaria Tocaci

Matter	Austria	Romania
Specific statutory provisions	Sections 48a to 48c of the Austrian Federal Fiscal Code; Sections 251 and 252 of the Austrian Criminal Tax Act.	Art 11 of the Romanian Fiscal Procedure Code; Art 227 of the Romanian Criminal Code; Art 46 of Law 188/1999 on civil servants.
Personal scope	Applies to civil servants and other persons (experts) participating in a tax or criminal tax proceeding.	- Applies to civil servants involved in tax administration and to experts designated by the tax authorities or by taxpayers to prepare expert reports. - Does not apply to tax advisors, who are bound by professional secrecy.
Material scope	Publishing or exploiting non-public information or circumstances of parties of tax or criminal tax proceedings that were disclosed or investigated in these proceedings.	Disclosure of information regarding taxpayers, eg tax liabilities, the amount and source of income, payments, account movements, deductions, debts, etc included in tax returns and in other documents disclosed by taxpayers or third parties.
Limit of scope	Use of information and circumstances (i) to carry out tax or criminal tax proceedings; or (ii) due to a legal obligation or compelling public interest; or (iii) obviously no interest worth being protected exists or the protected person consents; or (iv) to inform other authorities in case of suspicion that laws were violated (employment, social security, professional, trade, etc).	Use of information (i) to public authorities for fulfilling their obligations; or (ii) to tax authorities of other countries, based on the principle of reciprocity; or (iii) to judicial authorities; or (iv) to any requestor, with the written approval of the relevant taxpayer.
Civil consequences	Civil damage Civil injunction	Civil damage
Disciplinary or criminal consequences	- Disciplinary measures - Criminal Act: civil servants: up to 3 years prison, other persons: up to 6 months prison, daily fine up to 360 days.	- Disciplinary measures. - Criminal offence: up to 3 years prison, if the aggrieved person makes a complaint.
Consequences on the tax and criminal tax proceedings	- Published information may be used by the tax authorities. - Public may be excluded from tax or criminal tax hearings if they concern information or facts subject to tax secrecy.	- Information may be transmitted to the public when a final decision on breaching the tax legislation is reached, either in the administrative stage or in court. - In practice, tax secrecy does not apply in court; hearings on tax matters are generally public.
Relation between disclosure of information protected by tax secrecy and professional confidentiality	Professional confidentiality takes priority over tax disclosure obligations, even if protected by tax secrecy.	Professional confidentiality takes priority over tax disclosure obligations, unless the disclosure of the information is specifically requested by law.
Restriction of duty regarding professional confidentiality in regard to tax matters	In case of (criminal) tax proceedings against a person subject to professional confidentiality, such professional confidentiality may be restricted to the extent necessary to allow the tax authorities to examine and review the tax matters of that person (also in light of applicable tax secrecy).	A person subject to professional confidentiality is required to disclose information about the tax matters related to him, even if the information refers to matters which are under professional confidentiality. For example, in Romania all VAT registered taxpayers, including tax advisors, must periodically disclose via a special tax return information on the transactions carried out with their suppliers / clients.



Disclosure of tax planning schemes by intermediaries (proposal for an EU-Directive) Proposed date of application 1 January 2019

Theodor Artenie | Anamaria Tocaci

Cross-border tax arrangements bearing the tax avoidance hallmarks presented below should be notified by those intermediaries (tax advisors, accountants, lawyers, banks) who assist or advise on designing, marketing, organising or managing the tax relevant aspects of these arrangements. The reporting obligation could be waived for intermediaries if they are entitled to a legal professional privilege. If so, the obligation to file information on the arrangement will be the responsibility of the taxpayer. The information received will be exchanged automatically between Member States.

When a fixed percentage of the tax avoided is charged as fee, or when a fee is charged explicitly for tax avoidance services	Tax arrangements sold with a confidentiality clause attached
Providing arrangements which use losses to reduce tax liability	Providing tax avoidance advice that has been standardized and made available to more than one taxpayer
The same asset is subject to depreciation in more than one jurisdiction	Use of linked companies or entities with no substance and with circular transactions taking place between them
Converting income into other types of revenue which are taxed at a lower level	Deductible crossborder transactions based on the residency of the taxpayer
When mismatches occur between EU or national law and the taxation applied in a non-EU country	A payment mentioned in an arrangement is given a full or partial tax exemption in the jurisdiction where it should be taxed
Where the transfers of payment across borders do not represent the true value of the assets bought	Use of tax jurisdictions with no or low corporate tax rates, or which find themselves on the upcoming EU list of non-cooperative tax jurisdictions
Arrangements that re-classify income in categories not subject to automatic exchange of information agreements	Relief from double taxation on the same income in different jurisdictions by more than one taxpayer
Use of jurisdictions with inadequate or weak anti-money laundering rules, including those which help to conceal beneficial ownership information	Use of companies and entities not covered by EU rules or other agreements on automatic exchange of information
Arrangements which include reference to crossborder tax rulings that are not already being reported or exchanged	Arrangements that do not conform to the "arms' length principle" or to OECD transfer pricing guidelines

Source: http://ec.europa.eu/

Transfer pricing in Romania

Theodor Artenie | Anamaria Tocaci

- Even though Romania is not an OECD member, the OECD Transfer Pricing Guidelines are, in principle, recognised by the Romanian tax legislation.
- Still, there are certain particularities or additional information specifically required under local legislation as regards the transfer pricing documentation. A lack of information may trigger the risk that the Romanian tax authorities will consider the TP documentation incomplete. Presentation of incomplete TP documentation may lead to penalties and entitles the Romanian tax authorities to proceed with their own assessment of the taxpayer's transfer prices.
- Starting in 2016, large taxpayers – designated as such in a special order of the president of the National Agency for Fiscal Administration – which carry out transactions with related parties over certain thresholds, are required to prepare their transfer pricing documentation files on an annual basis.

Below is a summary of the transfer pricing obligations for Romanian taxpayers:

Who	When	Threshold	Deadline
Large taxpayers	No later than **the legal deadline for submitting the annual corporate tax return** for each fiscal year	**EUR 200,000** excluding VAT, for interest received / paid for financial services **EUR 250,000** excluding VAT, for supplies / acquisitions of services **EUR 350,000** excluding VAT, for sales / acquisitions of tangible or intangible goods	**10 days** from the request date
All taxpayers	Upon receipt of a written request from the tax authorities, as part of a tax audit	**EUR 50,000** excluding VAT, for interest received / paid for financial services or for supplies / acquisitions of services **EUR 100,000** excluding VAT, for sales / acquisitions of tangible or intangible goods	Between **30** and **60 days,** with the possibility to extend this term once by up to 30 days

For transactions carried out between Romanian companies and their associated foreign entities resident in other member states, the double taxation which might result following the adjustment of profits on one side should, in principle, be eliminated by means of corresponding mirror adjustments, based on the Convention on the elimination of double taxation in connection with the adjustment of profits of associated enterprises or based on bilateral double taxation treaties. The relevant procedure is yet to be defined in the Romanian legislation in this respect (ie mutual agreement procedure).

Space and privacy, space and time

In line with Makra's "Unified Fields" exhibition of 2017, Makra produced an abstract art piece specifically for Schoenherr, currently installed in one of the boardrooms in Vienna.

Insight into the discussion held between Guido Kucsko and Manfred Makra.

Makra immediately puts one at ease, and his calm temperament is in balance with his minimalistic art works which carry depth and beauty. Makra's take on privacy is truly edifying. When he talks about his relationship between individualism and community it becomes evident that he ultimately needs both. He examines the interplay between privacy and opening up, and the give and take of energy between people, between the energy of an artwork and the artist, and in turn, the audience.

With his understanding of privacy in mind, Makra always returns to the concept of space. Space and privacy, he believes are intertwined. Space, and what it holds are fundamental to his art. Where he creates; the space in which he creates.

When looking at a new space to create in, and in particular when he saw the Schoenherr boardroom for the first time, Makra describes how he assesses a room to determine how his "wall installations, wall paintings will resonate with the space." … "I try to get a feel for a room, the atmosphere of the room, and ask myself the first question: What does the room need? And I walked into this room which is wonderful, and I thought it needed a bit of soil, well the color of soil … and I thought it would be really nice to sit here and have a horizon in earth colors in front of you. And these colours go back historically to the first wall paintings."

Linking the way in which Makra approached Schoenherr's boardroom for his installation to the artwork he chose to create, the question of what art could mean in the context of being a manager arises. Makra believes "the most precious asset for a manager, is time. The calendars of managers are filled. The more entered, the more there is to be done. With an artist it is exactly the opposite. The less he has entered into his calendar, the more he can afford to devote himself to his art and to make something of quality. Here I see art as really supportive, because one thing is interesting, one can observe with oneself, if one creates space, whether it is a workspace or a private space, one always has the feeling that one also has more time. I've come to the point that people who have little sense of creating spaces, or creating outer spaces, or setting them up, that these people are more nervous and feel they have no time. When I experience space, time also expands. This is what I try to do with my installations, to have the effect that not only space expands, but also time."

That which is private and that which is open to scrutiny, it all boils down to a give and take of energy between people, between the energy of an artwork and the artist, and in turn, the audience. Art resonating in a space can allow one to focus, Makra's art certainly does: His art (and art generally) being a bridge reaching from the inside outwards, and from the outside in.

> Art is the bridge from the privacy of the artist to the privacy of the beholder.

Manfred Makra
Born in 1956 in Graz, Austria, Manfred Makra is the artist with whom we collaborated on the 2018 roadmap.

Makra started painting at age 19 after encountering the work of Antonio Caldera, the Italian painter who found inspiration in the lighting of landscapes, and who is known for his abstract works. As a result, Makra developed his own style using what he terms "contemplative colour", resulting in his exceptional works which he coins "poetry of the minimal."

Since 1990 Makra has frequently collaborated with international architects. A "zen aesthetic" influences his work, more profoundly so after his visits to Japan.

In his collaboration with us, Makra produced an artwork linked to and flowing from his "Unified Fields" exhibition of 2017. The series is clean, minimal and abstract, making use of balanced muted colours which elegantly tie in with the subtle geometry and spacial aspects used in his work.

Makra holds regular exhibitions throughout Europe, Japan, Australia and Dubai, and currently lives and works in Vienna, Austria.

For more information about the artist and his work please visit www.makra-art.com

credits

Imprint
© Schönherr Rechtsanwälte GmbH
Schottenring 19
A-1010 Vienna, Austria
T (+43 1) 534 37 - 0
F (+43 1) 534 37 - 66100
office.austria@schoenherr.eu
www.schoenherr.eu

Registration no. 266331 p, Commercial Court Vienna (Handelsgericht Wien)
UID: ATU 61980967
DVR: 157139

General information about roadmap18
Published and produced in Vienna, Austria
Management: Birgit Telsnig
Concept & Art Direction: Alfredo Suchomel
Coordinator & Editor-in-Chief: Liesel Beukes
Proofreader: Andre Swoboda.
Assistant: Carina Knowles
Art: Manfred Makra / www.makra-art.com
Manfred Makra is represented by Artmark Gallery, Vienna, Singerstraße 17 (www.artmark.at)
Photography: Nikolaus Korab: pages 1, 2, 4, 5, 12, 17, 18, 25, 26, 32, 36, 38, 43, 52, 62, 69, 72, 90, 94, 97, 100 / Alfredo Suchomel: pages 8, 28, 30, 48, 55, 59, 60, 70, 88, 104, 112, 114, 119, 127 / David Meran pages 122, 124, 125 / Susanne Einzenberger pages : 80, 83
Barcelona Chairs featured pages 122 & 123
Print & Production: Druckerei Jentzsch, Vienna

www.schoenherr.eu