MANZ'sche Verlags- und Universitätsbuchhandlung GmbH
TEL+43 1 531 61-11 FAX+43 1 531 61-99 hotline@manz.at
Johannesgasse 23, 1010 Wien www.manz.at

Spektrum

Dokumentinformation

Audit rights of the internal bank audit in cross-border situations (FN 1

Typ	Zeitschrift
Datum/Gültigkeitszeitraum	24.01.2019
Publiziert von	Jan Sramek Verlag
Autor	**Nicolas Raschauer** **Thomas Stern**
Fundstelle	**SPWR 2018, 113**
Seite	**113**

Abstract

Group Internal Audit is the central management instrument in banking groups. Its purpose is to identify weaknesses and risks in the operational and strategic areas, especially in banking groups operating across borders, analyse problems, develop suggestions for improvements to eliminate these weaknesses and ensure an efficient internal control system. In this way, Group Internal Audit supports the monitoring and control tasks of the parent company's management.

However, it is unclear to what extent the rights of inspection and information of the group's internal audit department apply and to what extent subordinate companies of the banking group are required to maintain confidentiality obligations. The following manuscript discusses the relationship between banking supervisory law and data protection law.

Inhaltsübersicht

Ende Seite 113

Anfang Seite 114»

Text

I. Background

The rapid increase in regulatory requirements in European banking supervision law has made internal audit (hereinafter ›IA‹), more than ever, a *third line of defense*. (FN [2]) In order to ensure a comprehensive control mechanism - also and in particular in banking groups - the auditors must have extensive access to all relevant business activities and processes.

This is all the more true the more complex the structure and activities of a banking group are, especially among subordinate companies abroad.

In the case of cross-border revisions in particular, the IA's inspection rights could diverge due to differing legal situations between the parent company and the subsidiary and, among other things, create problems for monitoring the consolidation.

The present article concretely addresses the rights and obligations of the **internal banking group audit** (hereafter referred to as »GA«) and focuses on the **inspection rights of this organizational unit in the course of its cross-border audit activities.**

II. Internal Audit - European legal framework

Despite its high practical relevance, the **role of IA** in the prudential supervision requirements at European level is mentioned explicitly either not at all (»CRD« (FN [3])) or marginal in the context of institution-specific calculation methods of regulatory standards (»CRR« (FN [4])). (FN [5])

The European legislator thus assumes (at least in specific cases) the existence of an IA, without, however, determining this function in European law. (FN [6])

From a systematic point of view, the IA forms **part of the »governance arrangements«** (art 74 para 1 CRD (FN [7])): Among other things, such arrangements must include **adequate internal control mechanisms** that take into account the nature, scale and complexity of the banking transactions carried out (paragraph 2 par cit).

According to CRD, the internal control mechanisms thus represent an **umbrella term** for the **process-dependent internal control system** (ICS) and the **process-independent IA.** (FN [8])

According to art 109 para 2 CRD (»application level«), appropriate internal control mechanisms should also be ensured at **(sub-)consolidated level.** (FN [9]) The

obligation to set up a **GA** thus results directly from art 74 para 1 **in conjunction with 109 para 2 CRD.**

III. Internal audit - Austrian legal framework

Pursuant to **art 42 para 1 of the Austrian Banking Act**, credit institutions and financial institutions have an *»internal audit unit which reports directly to the directors and which serves the exclusive purpose of ongoing and comprehensive reviews of the legal compliance, appropriateness and suitability of the entire undertaking«.*

In the Austrian Banking Act, the Austrian legislature explicitly distinguishes between ICS (art 39) and IA (art 42). (FN [10]) The separation is also clearly evident from art 39 para 2 last sentence of the Austrian Banking Act, according to which the IA has to check the *suitability and enforcement* of the ICS at least once a year.

Despite this structural separation, the requirement to establish an IA can be considered as part of the general due diligence obligations under art 39 of the Austrian Banking Act. (FN [11])

Within groups of credit institutions, the **superordinate institution** (IN) is responsible for fulfilling the tasks of the **GA** pursuant to art 30 para 5 of the Austrian Banking Act (art 42 para 7). (FN [12])

« Ende Seite 114

Zitiervorschlag

Anfang Seite 115»

In terms of corporate law, **art 82 of the Austrian Stock Corporation Act** and **art 22 of the Austrian GmbH-Law** require the establishment of an internal control system.

However, explicit requirements on setting up an IA are not found in company law. (FN [13])

However, art 92 para 4 no 4 lit b of the Austrian Stock Corporation Act requires the supervision of the internal audit system by the Audit Committee.

IV. Audit areas

The range of duties (audit areas) of the IA are partly prescribed by law (art 39 para 2 last sentence, art 42 para 1 and para 4 of the Austrian Banking Act, art 32 of the Austrian Securities Supervision Act 2018), but more specifically by market practices (FN [14]) and official expectations (FN [15]).

The examination of the **legal compliance, appropriateness and suitability** of the entire company (art 42 para 1 and para 4) and the ICS (art 39 para 2, art 42 para 4 no 5) includes the revision of all operating and business areas and processes of a CI (including anti-money laundering procedures and ICAAP/ILAAP), intrabank regulations and work instructions (FN [16]) including the auditing of accounting, risk assessment and data-processing systems (see art 32 of the Austrian Securities Supervision Act 2018). (FN [17])

For the **GA**, art 42 para 7 of the Austrian Banking Act does not standardize any explicit audit areas. (FN [18]) However, a purposeful orientation to the obligations under para 1 par cit seems reasonable to suppose by the law's mandate, according to which the IA of the superordinate institute has to take over the tasks of the GA, in conjunction with the relevant explanatory remarks of the government bill.

Thus, the purpose of the GA is to perform »the ongoing and comprehensive reviews of the legal compliance, appropriateness and suitability« of the entire **CI group** (art 42 para 1 analogously). (FN [19]) In accordance with the explanatory remarks of the

government bill of the original version of the Austrian Banking Act 1993 (FN [20]), the GA has **in particular** »to examine the formal and material regularity of the consolidated accounting, the compliance with the regulatory norms of this Federal Law and the advisability of the organizational structure of the Group«.

The phrase *»in particular«* clarifies the demonstrative character of this listing and leaves the GA sufficient room for interpretation as regards the materiality of the audit areas in the light of a risk-based auditing approach.

In our view, the obligation of the GA for **examination on a (sub-)consolidated level** (see art 39 para 2 in conjunction with art 42 para 7 of the Austrian Banking Act, or art 109 para 2 CRD and art 11 para 1 CRR) must be interpreted broadly in the light of effective and comprehensive auditing activities and must not be limited just merely to the abstract scope of consolidation (as

«Ende Seite 115

Anfang Seite 116»

a fiction of a whole organism neutralizing intra-group processes), but should also include, if appropriate, in other words taking account of the risk-based approach, audits at the solo level in the participations themselves. Otherwise, for example, the **audit of the IA at the subsidiaries by the GA** would not be guaranteed and the legal obligation for a comprehensive audit would not be fulfilled. However, the permissibility of such audits ends where the subsidiary's autonomy is disproportionately subverted. (FN [21])

V. Audit and inspection rights

Audit and inspection rights are not explicitly anchored in the Austrian Banking Act neither for the IA nor for the GA. However, in return, the relevant legal frameworks of the European banking supervision law serve as a template **for the GA's rights.** According to **art 1 09 para 2 first sentence CRD**, the institutions must ensure that *»arrangements, processes and mechanisms required by Section II* [general principles for internal control mechanisms according to art 74 CRD; note from the authors] *are consistent and well-integrated and that any data and information relevant to the purpose of supervision can be produced.«* (art 109 para 2 first sentence CRD).

Inversely, **art 11 para 1 CRR**, with explicit support for the *internal control mechanisms* to be set up by the institute, also stipulates an obligation for ensuring proper processing and forwarding the data necessary for (pillar I) consolidation. (FN [22]) Since **GA** forms part of the *internal control mechanisms*, it should also be granted access to all necessary data.

The **obligation to exchange information** applies to all companies in the scope of consolidation (FN [23]), irrespective of whether they are institutions in accordance with art 4 para 1 no 3 CRR in conjunction with art 2 CRD (see art 109 para 2 second sentence CRD).

Expressly stipulated is **the submission requirement** of all »data and information relevant to the purpose of supervision« at the expense of the subsidiaries (art 109 para 2 third sentence CRD), according to the wording, **irrespective of whether their seat is located in Austria, in the EEA or in a third country** (eg Switzerland, Serbia, USA, etc). (FN [24])

This includes the establishment of an effective reporting to ensure the required *look-through* at consolidated level. (FN [25])

The norm **is addressed** to **all regulated companies** included in the scope of consolidation. Similarly, art 11 para 1 second and third sentences CRR also applies to

the consolidating institution as well as to the consolidated (regulated) companies; they share responsibility for ensuring the exchange of information. (FN [26])

National legislators in the EEA must therefore not provide for any national provisions hindering an obligation to refer under art 109 para 2 third sentence CRD or art 11 para 1 CRR *(data ring fencing;* (FN [27]) see also art 124 para 1 CRD). *Argumentum a maiore ad minus* follows that seemingly conflicting national obligations of confidentiality to which a subsidiary is subject have to be interpreted in conformity with European law so that an exchange of information within the banking group is principally permissible in order to enable effective group management.

Thus, an exchange of information is ensured within the EEA in so far as the exchange concerns ***»data required for consolidation«*** (art 11 para 1 CRR) or ***»data and information relevant to the purpose of supervision«*** (art 109 para 2 first and third sentences CRD).

The wording of these provisions, in cases of doubt, suggests a very broad interpretation of the data concerned, as the aspects of the relevance is addressed both **internally** (art 11 CRR, »Prudential Consolidation«) and **externally** (art 109 CRD; »Review Processes«). Personal data (as a reference) as well as information covered by banking secrecy (art 38 of the Austrian Banking Act) are included in principle. (FN [28])

The problem of inapplicability of art 109 para 2 third sentence CRD and art 11 para 1 third sentence CRR **at the**

«Ende Seite 116

Anfang Seite 117»

solo level of subsidiaries in third countries is obvious, whereby the norm applies directly unilateral to the superordinate institute in the EEA. However, if the superordinate institute cannot guarantee the exchange of information, meaning if the GA does not receive all the necessary data from the company in the third country, **the institute violates its obligation under art 39 para 2 in conjunction with art 42 para 7 of the Austrian Banking Act at consolidated level** (violation of a pillar II provision). (FN [29])

Remarkably, this does not apply to pillar I consolidation, if the institution which is required to consolidate has been granted a license in accordance with art 19 para 2 lit a CRR (FN [30]) and thus, the third-country company is exempt from its scope of consolidation. **Essentially, participation in a consolidated company in a third country** which **cannot provide all the relevant data is inadmissible.** The **audit and inspection rights of GA are therefore to be fully and comprehensively ensured for participations also in third countries.**

VI. Interim summary

To summarize, both European and national legislators assume a consistent **congruence between the rights and obligations of GA.** Institutions must thus ensure that GA has the necessary audit and inspection rights for each audit area.

Within the CI Group, regulations which prevent the release of the necessary information to GA are inadmissible and would constitute a breach of the general due diligence obligations pursuant to art 39 para 2 and 7 in conjunction with art 42 para 7 of the Austrian Banking Act at the consolidated level. **This applies both within the EEA and in participations in third countries.**

VII. Group audit and European Data Protection Law

A. General

As shown, the **GA** should fulfill the following **task** (FN [31]) in particular: It is a guarantor of good corporate governance within the group due to its compulsory structure (art 42 para 7 of the Austrian Banking Act), risk manager and preserver of stakeholder interests, in other words of the claims of investors, clients, employees and the public - that is the role that not only the European legislator, supervisory authorities, financial investors, but also the public assigns to GA today.

The expectations of a GA are therefore high. Three out of four stakeholders believe that corporate scandals and economic criminality in recent years have increased the pressure on companies to set up a GA. (FN [32])

New legal requirements, stricter liability claims on directors (see, for example, art 65 ff CRD) and increasingly stricter external supervisory bodies have brought the previously outlined task of GA into sharper focus. Originally, GA as a mere monitoring body that randomly audited business transactions for proper accounting treatment, is now seen as a **key management tool** that identifies weaknesses and risks in the operational and strategic field - especially in European subsidiaries, that analyses problems, that makes suggestions for improvement to eliminate the weak points and that ensures an efficient ICS. Thus, **the GA supports the monitoring and control tasks of the management.**

B. Research question

Now, GAs in banking groups are increasingly confronted with the problem that European subsidiaries, but also third-party companies, deny the legally intended cooperation between parent companies and subsidiaries, for example at the level of information exchange (FN [33]). The array of **justifications** for the **refusal** of information exchange or cooperation ranges from privacy concerns about the lack of extraterritorial validity of the national banking law or corporate law to the lack of responsibility of GA for the verification of the conduct of the foreign subsidiaries.

Out of the group of **»denials«**, the **data protection law** stands out. Is it even permissible within a banking group for the entity to be inspected (a subsidiary) to refuse any information to the inspector (the GA) on

«Ende Seite 117

Anfang Seite 118»

the grounds of data protection concerns, if the initially outlined provisions of the European banking supervision law are left aside? »Prima vista«, the legal situation seems to be ambiguous, especially with regard to the **General Data Protection Regulation** (GDPR) (FN [34]), which has been in force since May 25, 2018.

We are confronted with an obvious **conflict of interest -** on the one hand is the management of the parent company of the banking group together with the GA, which is obliged to provide comprehensive due diligence and which has to control the entire group, including subordinate subsidiaries (art 38 and art 42 para 7 of the Austrian Banking Act, 84 of the Austrian Stock Corporation Act etc) - this requires a comprehensive insight into the events in the group and an ongoing *uninterrupted* flow of information between the group members.

On the other hand, subordinate CI - also and in particular in other European countries or third countries - are obliged to **maintain banking secrecy,** (FN [35]) or more generally: to maintain discretion in the interest of their clients, creditors, etc, as far as no obligation to provide information proceeds the (obligation of) confidentiality. (FN [36])

It has previously been shown that Austrian **company law does not help** in analyzing the relationship between GA and its subsidiaries, on the one hand, and directors, on the other hand, as far as the determination of **frameworks and barriers of the two-way exchange of information** is concerned. Although provisions of the type of art 247

para 3 of the Austrian Commercial Code (UGB) or art 30 para 8; art 42 of the Austrian Banking Act are characterized by the understanding that there is a principal obligation to provide information of the group-affiliated subsidiaries (including those outside the parent company's state of origin) to the parent institution and therefore also to GA. However, the objection of the lack of (local) validity of the mentioned rules outside the parent company's state of origin is obvious.

Therefore, the national company law cannot solve the mentioned cross-border conflict of interest satisfactorily. From the point of view of data protection law, an approach only results from the relevant European Union's primary and secondary law.

C. Excursus: Problem approximation based on supreme court rulings

While relevant, thematic European judicature (as far as can be ascertained) is lacking, the **Constitutional Court** (VfGH) has outlined a possible solution in a similar context, based inter alia on art 8 para 1 of the Charter of Fundamental Rights of the European Union (hereinafter: »Charter«), and makes clear statements about the **relationship between a controller's right of access** (here: the Committee of Inquiry of the National Council) **and those to be controlled** (in this case, the duties of presentation of the bodies of the Federation).

In the Selected Judgements of the Constitutional Court (VfSlg) 19.973/2015, the Constitutional Court summarized: It would not be possible to fulfill the inspection duties constitutionally conferred by the Committee of Inquiry without a comprehensive knowledge of *all files and documents* within the scope of the subject matter of the investigation. (FN [37])

In this limited scope of the object of investigation, limited by the duties of the Committee of Inquiry, the submission of the files and documents requested by the Committee of Inquiry would therefore be precluded by neither art 1 DSG nor art 8 ECHR and art 8 of the Charter. The same must apply all the more to the - **constitutionally interpreted -** basic legal provisions of **art 38 para 1 to 4 of the Austrian Banking Act** and art 48a of the Federal Fiscal Code (BAO).

Each institution subject to information must therefore present the **requested files and documents** unblackened (uncovered) to the extent of the subject matter of the investigation, **irrespective of other existing obligations of confidentiality.** (FN [38])

However, the obligation to provide **comprehensive information** to the body subject to the obligation to provide information would not have the power of the Committee of Inquiry or its members to publish the information obtained from the files or documents submitted, not even in the written report referred to in art 51 of the Rules of Procedure for Parliamentary Investigating Committees (RP-IC). Instead, the Committee of Inquiry regularly has **to balance interests** of its reporting between private secrecy interests (cf in this regard, art 1 DSG, but also art 8 ECHR and art 8 of the Charter) and public interests, which include, among others, the announcement of the results of the inspection. This bal-

«Ende Seite 118

Anfang Seite 119»

ance of interests is to be taken into account by the Committee of Inquiry in **all** its **activities.** (FN [39])

Due to functional comparability, this viewpoint can be transferred to the objective constellation.

D. Primary Law of the European Data Protection - art 7, 8 and 52 of the Charter

It should then be discussed whether the European data protection law contains specific **barriers to a comprehensive exchange of information** between parent company/GA and subordinate subsidiaries in a banking group. (FN [40])

The investigation is limited to **art 8 in conjunction with art 52 para 1 of the Charter;** Art 7 of the Charter as well as comparable provisions in the ECHR or in the national art 1 DSG are not dealt with separately. On the one hand, the prevailing opinion (FN [41]) is that art 8 of the Charter is lex specialis in relation to art 7 of the Charter; thus, the ECJ applies primarily to art 8 of the Charter as a standard of interpretation in data protection cases. (FN [42]) On the other hand, art 7 of the Charter and art 8 ECHR as well as art 1 DSG are similar (apart from the barriers that are once more narrowly, once more open ended formulated for intervening in fundamental right). (FN [43])

However, while the direct applicability of art 8 of the Charter by a parent company of a banking group, as evidenced by art 51 para 1 of the Charter (FN [44]), is not an option, specific requirements can be derived from the national legislator from the above-mentioned provisions of art 8, art 52 para 1 of the Charter, if the national legislator legally complements the data processing, inter alia, by private sources or questions of information transmission.

A (specific legal) restriction or further elaboration of the fundamental right of data protection laid down in art 8 para 1 of the Charter is only permitted in accordance with the general intervention limits pursuant to art 52 para 1 of the Charter. (FN [45])

According to this standard, the restriction (forming) of the fundamental right guaranteed by art 8 of the Charter is subject to

- the general formal limitations of art 52 para 1 first sentence of the Charter: Any interference with the fundamental right of art 8 of the Charter - either by national law or by Union legislation (see art 51 para 1 of the Charter) - requires an **explicit legal basis** (FN [46]) and must not infringe the guarantee of intrinsic nature of art 52 para 1. (FN [47]) It covers, for example, the le-

«Ende Seite 119

Anfang Seite 120»

gal transfer of the authorization to process personal data to a private entity such as a GA.

- the specific material limitations of art 52 para 1 in conjunction with art 8 para 2 of the Charter: Any interference, including the transfer of the power to process personal data to a private entity (such as the GA), must comply with the **principle of proportionality**, which means that the interference is in the public interest, appropriate to achieve the objective and necessary (FN [48]) and ultimately, appropriately done (FN [49]). However, a corresponding expression of this principle must be directly contained in art 8 para 2.

In other words, an exchange of information within the banking group or the processing of personal data by the GA by means of concrete statutory authorization within the meaning of art 8 of the Charter is permitted, if the aforementioned conditions are met on a case-by-case basis.

If the GA does not have a *concrete* statutory authorization to process data, but only a general allocation of tasks pursuant to art 42 of the Austrian Banking Act, (FN [50]) an exchange of information or **data processing** in the banking group is **permitted**, if (FN [51])

- it is done (FN [52]) in good faith (FN [53]), that is, for a **legitimate purpose** (FN [54]) (on the performance of the task assigned according to art 8 para 2 first sentence first alternative of the Charter); the subject-matter of the collection of personal data must

be determinable in this context (the objective of collecting and processing the data must be as precise as possible); and

- the **party concerned**, whose data is processed, expressly agrees (FN [55]) with the data processing in the knowledge of the state of the data processing (art 8 para 2 first sentence second alternative of the Charter); this consent may be granted only for the specific case and not on a flat-rate basis, furthermore it can only be granted for a specific purpose and does not cover future changes of the purpose.

Should the person whose data is being processed refuse to consent to processing - that is, among others, intra-group exchange of information - **data processing is also permitted** if, on the one hand, this is - in the concerned case - **necessary** in order to fulfill the task and, on the other hand, to **fulfill certain legitimate interests.**

This last (third) alternative is not expressly provided for in art 8 para 2 of the Charter, (FN [56]) but could be covered in the last alternative of art 8 para 2 (»or some other legitimate basis laid down by law (FN [57])«). (FN [58])

Consequently, if none of these conditions at the time of data processing are met, there is a breach of the fundamental right under art 8 of the Charter. Even the mere unlawful communication of personal data in the banking group can be considered as such an infringement. It is irrelevant whether the processing also leads to the detriment of the persons concerned (FN [59]) or whether the information is to be regarded as sensitive (FN [60]).

It is a consequence of the above that **art 8 para 2 of the Charter** itself formulates specific (directly applicable) **barriers** (throughout the EEA) to the statutory fleshing out of the **information exchange** in the banking group between subordinate subsidiaries and GA. Therefore, if in the case that there is no consent of the party concerned for data processing, another *generally held statutory task* - such as art 42 of the Austrian Banking Act - may empower or require the GA or art 39 of the

«Ende Seite 120

Anfang Seite 121»

Austrian Banking Act the management to obtain, review and process all relevant information including personal data in the interest of an effective group management.

The above-mentioned prudential authorization standards of the **Austrian Banking Act** thus **legitimize** the **processing of personal data** in the sense of the above. The decision as to what is required in this context, that is to say which data is to be processed, is made by the GA or the management, but not by any other group entity subject to the information obligation. (FN [61])

In principal, **entities subject to this information obligation** in the banking group could therefore not rely on seemingly conflicting confidentiality provisions such as the national banking secrecy and the like. As has been shown, the latter provisions must be interpreted - in conformity with European and Constitution Law (FN [62]) - in such a way that they do not preclude an exchange of information *in the interests of effective, cross-border group management.*

E. Secondary Law of the European Data Protection

No other assessment can be made if one considers the GDPR which has been in force since May 25, 2018.

Art 6 para 1 GDPR, under the heading **»Legality of processing«**, states that the processing of personal data by responsible persons or processors is only lawful on a case-by-case basis, if at least one of the following conditions is met:

a. the party concerned has given his consent to the processing of the personal data concerning himself for one or more specific purposes;

b. the processing is necessary for the performance of a contract to which the person concerned is a party, or for the performance of pre-contractual measures which are carried out at the request of the person concerned;

c. the processing is necessary to fulfill a legal obligation to which the responsible person is subject;

d. the processing is necessary to protect the vital interests of the person concerned or any other natural person;

e. the processing is necessary for the performance of a task in the public interest or in the exercise of official authority delegated to the responsible person;

f. the processing is necessary to protect the legitimate interests of the responsible person (FN [63]) or a third party, unless the interests or fundamental rights and freedoms of the person concerned, who requires personal data protection, prevail, especially if the person concerned is a child. (FN [64])

In that regard, **art 6 para 3 GDPR** states that the **legal basis** for data processing, which is based on art 6 para 1 lit c and e, should be established by Union or national law to which the responsible person (FN [65]) is subject.

It is also necessary that the **purpose of the processing** should be **laid down** (FN [66]) in this legal basis.

In addition, art 6 para 3 GDPR provides that the Union or the law of the Member State which legitimates data processing must **pursue a public interest objective** and must be **proportionate to the legitimate purpose pursued.**

Art 6 para 1 lit c and **f** GDPR (argumentum **»For the protection of legitimate interests«; »performance of a task...«)** stands out of the group of previously listed facts which could legitimize an exchange of information in the banking group and the processing of personal data by the GA on a case-by-case basis.

1. In particular: Art 6 para 1 lit c and f GDPR as the legal basis for the exchange of information in the banking group

In principle, data processing and the associated exchange of information in the banking group are permissible according to art 6 para 1 lit c GDPR if the person responsible (here: the parent company of a banking group) is subject to a legal obligation in the kind of art 42 para 4 no 3 of the Austrian Banking Act (Verification of Compliance with the Financial Markets Anti-Money Laundering Act (FM-GwG)) and the data processing is required *in this context* - here: keyword effective group management. (FN [67])

However, what has to be regarded as a **legitimate interest** when referring to art 6 **para 1 lit f** GDPR is not expressly determined by that provision. The term is clearly wider than that of »vital interest« within the meaning of art 1 para 1 lit d. All in all, there is strong evidence that the »legitimate interest«, as set out in art 6 para 1 lit f GDPR, is **any** (legitimate, recognizable) **intrinstic, economic or legal interest of the responsible person** or a third party. (FN [68])

«Ende Seite 121

Anfang Seite 122»

Therefore, for example, the obligation of the parent company (its management) or GA pursuant to art 42 of the Austrian Banking Act is to investigate or to solve suspected cases or to counteract them in a preventive manner, that could justify the processing of personal data or the intra-group exchange of information. (FN [69])

2. Relevance of European data protection law in third countries

As explained earlier in section 5, it was stated that all regulated companies in the scope of consolidation, in other words all subordinate subsidiaries of the banking group, irrespective of their place of residence, are the addressee of the information and disclosure rights conferred on to GA. It could be argued that European data protection law is not relevant in third countries (eg Switzerland, USA, Serbia etc) and that subsidiaries from third countries are not subject to the obligation to inform their European parent company. (FN [70])

As far as the Charter is concerned, this objection is, at least prima vista, not unjustified. It follows from art 51 para 1 of the Charter that the Charter is not applicable in third countries. However, nothing can be gained from this provision in order to resolve the issue of the territorial scope of the European data protection law or the subsidiary's obligation to provide information, since the Charter inter privatos is not directly applicable and art 8; 52 para 1 of the Charter only contains requirements for the forming of the fundamental right to data protection by bodies of the European Union and the Member States. According to art 52 para 1 of the Charter, however, it remains questionable how legal specifications which are laid down in art 8 of the Charter and which authorize the GA to exchange information and to process personal data also with regard to subsidiaries in third countries (cf, for example, art 109 CRD; art 42 of the Austrian Banking Act) are to be seen.

Art 3 para 2 GDPR brings some light into the darkness. According to this provision, the GDPR is also applicable in those third countries in which subordinate subsidiaries of a banking group are located: This applies on condition that the subsidiaries process data from bank clients who are in the European Union, and that they have offered their clients services, for example, or have observed and evaluated their behavior.

If the GDPR is also applicable from the perspective of the third-country subsidiary, the transmission of information to the parent company in accordance with art 6 para 1 GDPR cannot be refused on the ground of the lack of application of the GDPR or on the ground of the obligation to secrecy.

However, if one reaches the interpretation on a case-by-case basis that the GDPR is not applicable in the third country, because it is of the scope of art 3 para 2 GDPR, the problem cannot be resolved, at least at the level of existing European data protection law: The GDPR is not applicable in the third country. However, from a teleological point of view, this objection (hence the appeal of the third-country society to the lack of application of the GDPR in the third country) is wrong. The third-state subsidiary cannot simply overplay its obligations under company and banking supervision law towards its European parent company and its direct link to European data protection law or the GDPR; such an approach would be clearly unlawful or legally abusive.

Therefore, in order to solve this problem - the GDPR and specifically European secondary law applies directly on one side only to the superordinate parent company in the EEA - it is necessary to refer to section 5 and the requirements of European banking supervision law. Since, as has been shown, the European parent company is obliged to any other sanction to ensure the exchange of information in the banking group and also to enforce it against non-European subsidiaries (see, for example, art 70 of the Austrian Banking Act), the third-party subsidiary is not entitled to invoke the lack of applicability of European data protection law in the third state in the interests of effective group management or the ability to function in prudential consolidation. Such an objection would clearly be unlawful in individual cases and should be rejected, especially since the European parent company is subject to the obligations of the European banking supervision law; the public interest in the effective management of the banking group, its ability to function as well as the effectiveness of the supervisory consolidation must, as a result, be subject to data protection concerns of the subsidiary. This therefore leads to the assessment that a third-party subsidiary must also be bound to the requirements of European data protection law at least indirectly, because only in this way an intra-company exchange of information could be guaranteed.

However, if the subsidiary continues to refuse to cooperate, the European parent company will only have the option to review the closing of the third-country-participation in order to avoid penalties by the national Financial Market Supervisory Authority.

F. Second interim summary

Looking at the legal bases of the Austrian Banking Act and the CRD/CRR quoted above, the purpose of the provisions - **effective and comprehensive group manage**

«Ende Seite 122

Anfang Seite 123»

ment - is clear. The management of the parent company of the banking group has to use, inter alia, GA for this purpose. This instance can fulfill its task (see above II, VII.A.) only if it has **broad access to all relevant information** in the context of the principle of proportionality (as it is also the case in art 5 para 1 GDPR) and if it decides on its own which information is to be provided and which personal data is to be processed.

Vice versa, all subordinate group units (including third countries) are therefore required to cooperate fully with the parent company management and GA. They must submit the requested information in an editable format within a reasonable period. Therefore, an exchange of information may not be stopped at an internal border in the sense of effective corporate control.

In the sense of the Selected Judgements of the Constitutional Court (VfSlg) 19.973/2015, apparently **conflicting national confidentiality obligations** (related to the legal systems of subordinate group units, such as bank secrecy) to which a subordinate unit is subject must be interpreted in conformity with European and constitutional law in such a way that an **exchange of information or data processing takes place to/by the parent company or the GA.**

A contrary interpretation to the effect that the confidentiality obligations of the subordinate group entities would proceed with the exchange of information fails to recognize the fact that **confidentiality obligations are not** guaranteed **without its limits.** It is therefore not surprising that the Selected Judgements of the Constitutional Court (VfSlg) gave priority to the information interest and the audit of the National Council's Committee of Inquiry in a comparable context. Transferred to this case: **Confidentiality obligations of subordinate group units therefore have to withdraw in the interests of an effective group management.**

This »distribution of roles« is based on a (permanent) reconciliation of interests as the Selected Judgements of the Constitutional Court (VfSlg) has recognized in its result. For statutory controls (within the meaning of art 42 para 4 of the Austrian Banking Act) to work, the task of balancing interests - which information is relevant to the investigation and are therefore requested; which data are to be processed in the interests of an effective group management - is settled by the controller, but not by the group units to be controlled.

If one were to structure the mentioned distribution of roles differently and put the case for the primate of the confidentiality obligations of the subordinate group companies, any required prudential group control would fail. Such an outcome of the interpretation is not convincing.

This is not to say that the confidentiality obligations to which subordinate group entities are subject are »worthless« or »devoid of meaning ». However, according to the opinion of the management of the **parent company or the GA**, the parent company or the GA **is responsible** for »incidentally considering« or protecting the confidentiality obligations and, for example, processing only those personal data which are absolutely necessary for the fulfillment of the statutory controls.

VIII. Summary

The GA is *the* central management tool in banking groups. It should - especially in cross-border banking groups - identify weaknesses and risks in the operational and strategic field, analyze problems, recommend improvements to combat the vulnerabilities and ensure efficient ICS. Thus, the GA supports the monitoring and control tasks of the parent company's management.

In order for the GA to be able to fulfill its tasks envisaged, subordinate group companies of the GA have to provide the necessary documents and information upon request. Confidentiality obligations to which the companies are subject take second place to the right of information of the GA due to the existing legislation (CRD, CRR, art 42 of the Austrian Banking Act, art 6 para 1 lit c and f GDPR, art 7, art 8 para 2 and art 52 para 1 of the Charter).

IX. Bibliography

Article-29-Working Party, Opinion 06/2014, 844/14/EN (2014).

BCBS, The internal audit function in banks (2012).

EBA, Guidelines on internal governance (EBA/GL/2017/11) 2017.

EBA, Opinion of the European Banking Authority on the application of articles 108 and 109 of Directive 2013/36/EU and of Part One, Title II and article 113(6) and (7) of Regulation (EU) No 575/2013 (EBA/Op/2014/11) (29. 10. 2014).

FMA Austria, FMA Minimum Standards for Internal Auditing (FMA-MS-IR) (18. 2. 2005).

FMA Austria, F FMA Minimum Standards for the Preparation of an Emergency Concept within the meaning of art 30 of the Austrian Investment Fund Act (InvFG) 2011 and art 39 of the Austrian Banking Act (1. 9. 2011).

FMA Austria, FMA Minimum Standards for the Risk Management and Granting of Foreign Currency Loans and Loans with Repayment Vehicles (FMA-FXTT-MS) (1. 6. 2017).

Höllerer/Puhm/ Stern in Dellinger, Austrian Banking Act-Comment (2017) art 39.

«Ende Seite 123

Anfang Seite 124

Keinert, Organization of internal audit, in particular possibilities of outsourcing according to art 42 para 6 Austrian Banking Act, ÖBA 2011, 81.

Kessler in Dellinger (ed), Austrian Banking Act-Comment (2016) art 42.

Kingreen, art 8 and 52 Charter, in *Calliess/Ruffert* (eds), TEU/TFEU[5] (2016).

Meeuwsen, Establishment of an internal audit using the example of a group audit in Amling/Bantleon (eds), Practice of Internal Auditing (2018) 177.

Mikulik in Laurer/M. Schütz/Kammel/Ratka (eds), CRR-Comment (2017) art 368 CRR.

Öhlinger/Eberhard, Constitutional Law, 10. edition, 2016.

B. Raschauer, Federation - Administration - Institution, JRP 2017, 110.

N. Raschauer /Riesz, art 8 in Holoubek/Lienbacher (eds), Charter (2014).

N. Raschauer, The fundamental right to data protection of the European Charter of Fundamental Rights and its relationship to the ECHR and the national fundamental order

in Bammer et al (eds), Legal protection yesterday - today - tomorrow, FS Machacek/Matscher (2008) 381.

Reimer, art 6 in Sydow (ed), GDPR (2017).

Schirk/ Stern in Laurer/M. Schütz/Kammel/Ratka (eds), Austrian Banking Act/CRR-Comment (2017) art 11, 18.

Schmidbauer/Ziebermayr in, Laurer/M. Schütz/Kammel/Ratka (eds), Austrian Banking Act/CRR-Comment (2017) art 42.

Siegl, FMA Minimum Standards for Internal Auditing (»FMA-MS-IR«), ÖBA 2005, 742.

Stern in Laurer/M. Schütz/Kammel/Ratka (eds), Austrian Banking Act/CRR-Comment (2017) art 19.

Zitiervorschlag

Zum Autor

Prof. Dr. Nicolas Raschauer, Propter Homines Lehrstuhl für Bank- und Finanzmarktrecht, Institut für Wirtschaftsrecht, Universität Liechtenstein, Fürst Franz Josef Strasse, 9490 Vaduz. Mail: finanzmarktrecht@uni.li, Tel: +423 - 265 11 11.

MMag.Dr. Thomas Stern, MBA, Finanzmarktaufsicht Liechtenstein, assoziierter Wissenschaftler an der Universität Liechtenstein. Mail: finanzmarktrecht@uni.li, Tel: +423 265 11 11

Fußnote(n)

1) Das gegenständliche Manuskript wird parallel in deutscher Sprache im Österreichischen Bankarchiv veröffentlicht.

2) See among others *Schmidbauer/Ziebermayr* in Laurer/M. Schütz/Kammel/Ratka (eds), Austrian Banking Act/CRR Comment (2017) art 42 recital 59.

3) Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, OJ 2013 L 176 / 335.

4) Regulation (EU) no 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) no 648/2012, OJ 2013 L 176/1. »References« to the IA can be found in art 191, 221 para 4 lit h, 225 para 3 lit d, 259 para 3 lit g, 228, 292 para 1 lit f, 293 para 1 lit h, 321 lit e, 368 para 1 lit CRR; in most cases, these references are made in the context of internal models.

5) cf *Kessler* in Dellinger (ed), Austrian Banking Act Comment (January 2016) art 42 recital 13; *Schmid-Bauer/Ziebermayr*, art 42 recital 12.

6) As a requirement, only in art 368 para 1 lit d (nicht e) CRR the sufficient number and the fitness of the auditing staff in connection with the audit of internal models is required; see *Mikulik* in Laurer/M. Schütz/Kammel/Ratka (eds), CRR Comment (2017) art 368 CRR recital 2.

7) Emphasis not in the original.

8) cf also EBA, Guidelines on internal governance (EBA/GL/2017/11) 198.

9) cf also EBA, Guidelines on internal governance (EBA/GL/2017/11) 199.

10) cf also art 25a para 1 no 3 of the German Banking Act: The norm explicitly divides *internal control procedures* into ICS and, separately, IA.

11) *Höllerer/Puhm/ Stern* in Dellinger (ed), Austrian Banking Act Comment (2017) art 39 recital 14.

12) The parallel obligation of establishing an ICS and IA also at the consolidated level (art 30 para 7, art 42 para 7 of the Austrian Banking Act) is systematically consistent and, it is - in terms of the level of application of art 74 para 1 in conjunction with art 109 para 2 CRD - also in conformity with the Directive. The functional assignment of the tasks of the GA to the subordinate CI standardized in art 42

para 7 of the Austrian Banking Act should, however, be viewed as quite flexible by the legislature. For instance, art 42 para 6 continues to permit the waiving of separate organisational unit on a solo basis, if *»provided that a separate organisational unit for internal audit exists* within the group *[highlighting by authors] of credit institutions or the sectoral association, of the credit institution group or sector federation a separate organizational unit for internal audit exists«* (last expanded by Austrian Federal Law Gazette I, no 149/2017); see *Keinert*, organization of the internal audit, in particular possibilities of their outsourcing according to art 42 para 6 of the Austrian Banking Act, ÖBA 2011, 81.

In contrast to art 42 para 7, art 42 para 6 last subparagraph thus seems to assert cases in which the GA may also have a decentralized-functional character *(»within the group«).* Already the explanatory remarks of the government bill to the Austrian Federal Law Gazette 1993/532, 1130 BlgNo 18th GP 144, justified the functional allocation to the subordinate CI exclusively with their *practicability.* In order to resolve this supposed contradiction, it can be assumed that the GA (in the superordinate CI) may functionally use the IA in the respective (subordinate) entities (as vicarious agents of the GA), as long as this increases the effectiveness and efficiency of the audit activities and neither leads to self-assessment/internal audit nor to other potential conflict of interest. cf also Kessler, art 42 recital 122; see also *Keinert*, ÖBA 2011, 81. Especially in more complex structures, such as in multi-level CI groups or sector networks, it should be fundamentally permissible for subordinate or assigned institutes to act functionally in relation to other subordinate entities as GA under the above-mentioned conditions. However, the responsibility always remains with the superordinate CI.

13) cf *Schmidbauer/Ziebermayr*, art 42 recial 14.

14) See, for example, BCBS, The Internal Auditing Function in Banks (2012).

15) See *FMA Austria*, FMA Minimum Standards for Internal Auditing of February 18, 2005 (FMA-MS-IR); *FMA Austria*, FMA Minimum Standards for the Risk Management and Granting of Foreign Currency Loans and Loans with Repayment Vehicles of June 1, 2017 (FMA-FXTT-MS) recital 9; *FMA Austria*, FMA Minimum Standards for the Preparation of an Emergency Concept within the meaning of art 30 of the Austrian Investment Fund Act (InvFG) 2011 and art 39 of the Austrian Banking Act (September 1, 2011) recital 2.

16) cf *FMA Austria*, FMA Minimum Standards for Internal Audit (FMA-MS-IR); *Siegl*, FMA Minimum Standards for Internal Audit (»FMA-MS-IR«), ÖBA 2005, 742; *Schmidbauer/Ziebermayr*, art 42 recital 54 f.

17) For details on the obligations in performing the audit see *Schmidbauer/Ziebermayr*, art 42 recital 72 ff; *Kessler*, art 42 recital 45 ff; and *EBA*, Guidelines on internal governance (EBA/GL/2017/11) recital 201 ff.

18) cf also *Siegl*, ÖBA 2005, 742. However, a list of the tasks of the GA can be found, inter alia, in *Kessler*, art 42 recital 120.

19) It is also irritating that art 42 para 7 of the Austrian Banking Act prominently uses the term »group«, but the obligation to set up a GA addresses the (potentially narrower) credit institutions group pursuant to art 30 of the Austrian Banking Act (see art 30 and 59 of the Austrian Banking Act); See also *Schirk/ Stern* in Laurer/M. Schütz/Kammel/Ratka (eds), Austrian Banking Act/CRR Comment (2017) art 18 CRR recital 20 f.

20) cf explanatory remarks of the government bill 1130 Austrian Federal Law Gazette BlgNo 18. GP 144 (f.n. 12).

21) cf *Schmidbauer/Ziebermayr*, art 42 recital 113. Since K-IR operates in the interests of the group and is obliged to carry out a comprehensive audit, it is to be assumed that K-IR has a extensive guideline competence vis-à-vis the subordinate IRs (e.g. specification or supplementation of certain audit topics and audit methodologies). To ensure the consistency of the group-wide auditing activities, the K-IR has also a quality assurance function on a regular basis (e.g. when finalising audit reports).

22) cf *Schirk/ Stern* in Laurer/M. Schütz/Kammel/Ratka (eds), Austrian Banking Act/CRR comment (2017) art 11 CRR recital 25 ff.

23) cf *EBA*, Guidelines on internal governance (EBA/GL/2017/11), recital 82.

24) Nor is it undermined by art 109 para 3 CRD, according to which the rules on internal company management and control (Title VII, Chapter 2, Section II, CRD) do not apply to subsidiaries in third countries if the superordinate institution can prove the illegality of the application of these requirements in the third country (see *EBA*, Guidelines on internal governance [EBA/GL/2017/11], recital 87). The obligation to disclose data is based on section V (art 109 para 2 CRD), however, and is not restricted by art 109 para 3 CRD.

25) cf *Schirk/ Stern*, art 11 recital 8.

26) The competent authority could therefore require both from the consolidating institution and from the institution that holds the participation directly the establishment of the lawful state of affairs under art

70 para 4 no 1 of the Austrian Banking Act. The obligation shall only not apply to companies that have been removed from the scope of consolidation pursuant to art 19 CRR; see *Schirk/ Stern* , art 11 recital 28.

27) National banking secrecy rules should not hinder prudential consolidation.

28) cf *Schirk/ Stern* , art 11 recital 27.

29) In such a case, ensuring the exchange of information would have to be examined basically in advance by the FMA, provided that the company in the third country is an CI (approval according to art 21 para 1 no 2 of the Austrian Banking Act), see *Stern* in Laurer/M. Schütz/Kammel/Ratka (eds), Austrian Banking Act/CRR Comment (2017) art 19 recital 14.

30) This normative extension of the De-Minimis rule actually seems surprising to a prudential regime, but has **no relevance** in practice. cf *Stern* , art 19 recital 11 ff. The EBA even proposed a deletion of lit a in 2014, but so far has been unheard of by the European Commission (also taking into account the proposals for CRR II). cf also *EBA*, Opinion of the European Banking Authority on the application of Articles 108 and 109 of Directive 2013/36/EU and of Part One, Title II and Article 113(6) and (7) of Regulation (EU) No 575/2013 (EBA/Op/2014/11) (29. 10. 2014).

31) For this purpose, see *Meeuwsen*, Setting up an Internal Audit using the Example of a GA in Amling/Bantleon (eds), Practice of Internal Audit (2018) 177 ff.

32) *Meeuwsen* (f.n. 31) 177.

33) There is a special form of data transfer (disclosure) between different group units (cf art 4 no 2 GDPR).

34) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

35) Exceptions confirm the rule: see, for example, Germany, which got rid of banking secrecy by July 23, 2017 (repeal of art 30a of the German Act to Combat Tax Evasion (dt StUmgBG)).

36) cf general provisions of the type of art 6 para 1 DSG (data secrecy) and art 38 para 1 of the Austrian Banking Act (banking secrecy) and similar provisions in other EEA and third countries.

37) cf also Selected Judgements of the Constitutional Court (VfSlg) 4106/1961 in connection with the audit mandate of the Court of Auditors.

38) cf Selected Judgements of the Constitutional Court (VfSlg) 17.065/2003 and 19.834/2013 for procedures under art 126a of the Federal Constitutional Law (B-VG).

39) It should not be overlooked that this knowledge was criticized in the literature (cf instead of many *B. Raschauer* , Federation - Administration - Institution, JRP 2017, 110 [116 f]). However, the criticism refers less to the interpretation of the Court in the above-mentioned finding concerning the obligation to provide information by legal entities, but rather on the apparent incorrectly drawn circle of institutions which have a duty to submit (according to art 53 of the Federal Constitutional Law (B-VG)) per se (especially as lent or outsourced legal entities do not belong to the institutions which have a duty to submit (Selected Judgements of the Constitutional Court (VfSlg) 19.903/2015).

40) cf section VII.E.2 for the local area of application of the Charter.

41) cf, for example, *N. Raschauer /Riesz*, art 8 recital 5 in Holoubek/Lienbacher (eds), Charter (2014); *Kingreen*, art 8 recital 1 in Calliess/Ruffert (eds), TEU/TFEU[5] (2016).

42) See only ECJ 21. 12. 2016, C-203/15 and C-698/15 (Tele2 Sverige AB), ECLI:EU:C:2016:970.

43) cf, for example, Selected Judgements of the Constitutional Court (VfSlg) 19.892/2014; *N. Raschauer /Riesz*, art 8 recital 6 in Holoubek/Lienbacher (eds), Charter (2014).

44) Thereafter, the Charter applies only to the institutions of the Union and to those of the Member States in the implementation and application of Union law, but not (directly) inter privatos (art 51 para 1 of the Charter).

45) cf *N. Raschauer* , the fundamental right to data protection of the European Charter of Fundamental Rights and its relationship to the ECHR and the national fundamental order in Bammer et al (eds), FS Machacek/Matscher (2008) 381 (396 f); continuing with *N. Raschauer /Riesz*, art 8 recital 21 f in Holoubek/Lienbacher (eds), Charter (2014). Article 52 para 2 and 3 of the Charter are not relevant in the present context: First, as is clear from art 52 para 2 of the Charter, the rights recognized by the Charter - consequentially also the fundamental right to data protection, if and insofar as it is provided for by the EU treaties, that is to say regulated in primary law - takes place within the conditions and limits laid down therein. This does not help in the context of interest here, as no explicit limits are

formulated in the Union Treaties, see art 39 TEU and art 16 TFEU. This leads to only one conclusion, namely that art 52 para 2 of the Charter is not applicable in this case.

Furthermore, art 52 para 3 of the Charter shall not be considered either. This can be explained by the fact that art 8 ECHR does not contain any explicit data protection-specific regulations. Rather, art 8 of the Charter - thus also the Explanatory Notes on the Charter - shall be qualified as an independent fundamental right, which means that art 8 of the Charter is not an »ECHR accessory fundamental right« and consequently the ECHR's barriers to art 8 of the Charter are not applicable. It can therefore be concluded that in the absence of applicability of para 2 and 3, the general intervention clause laid down in art 52 para 1 shall apply to the assessment of an encroachments on the fundamental right to data protection evaluation pursuant to art 8 of the Charter; cf *N. Raschauer /Riesz*, art 8 recital 14 in Holoubek/Lienbacher (eds), Charter (2014).

46) This legal reservation is to be interpreted broadly. What is ultimately considered a »legal basis« does not follow from the Charter. It will therefore be necessary to differentiate between Union and Member State measures. In the case of doubt, one of the legal principle of art 288 TFEU will be used at Union level, as far as an encroachment on the fundamental right of data protection is to take place. At Member State level, then, national constitutional principles will prevail. In this context, it should be noted that the Member States/the Union must detail all measures authorizing encroachments on the fundamental right (therefore a high degree of determination is required; rather than many, see, for example, ECtHR 1. 7. 2008, *Liberty*, appl 58243/00).

47) cf the explanatory remarks on art 52 of the Charter based on the ECJ 13. 4. 2000, C-292/97, *Karlsson* recital 45. What could be the intrinsic nature of art 8 can only be determined in a specific case by considering the options. It should be noted at this point that encroachments that equal the »abolition« of the fundamental right are in any case inadmissible. See, for example, *Öhlinger/Eberhard*, Constitutional Law (2016) recital 713.

48) For the interpretation of the concept of necessity from the perspective of the law of the Union, cf, for example, ECJ 14. 12. 2008, C-524/06, *Huber*, ECLI:EU:C:2008:724, recital 52, 58 f.

49) An encroachment is necessary if it is to pursue an EU objective that is genuinely in the public interest, or to protect the individual rights of third parties (such as life or health). cf *Kingreen*, art 52 recital 67, in *Calliess/Ruffert* (eds), TEU/TFEU[5] (2016).

50) From the point of view of the GA, for instance, to check compliance with the Financial Markets Anti-Money Laundering Act (FM-GwG) (MLA) in the banking group (art 42 para 4 no 3 of the Austrian Banking Act).

51) cf *N. Raschauer /Riesz*, art 8 recital 14 in Holoubek/Lienbacher (eds), Charter (2014).

52) The purpose of the data collection or the processing must be established even before the collection itself. A subsequent change is only permissible, if it is compatible with the original purpose *(N. Raschauer /Riesz*, art 8 recital. 14 in Holoubek/Lienbacher [eds], Charter (2014).

53) This requirement for the admissibility creates a catch-all clause in order to be able to qualify processing data as unlawful even in the absence of a corresponding statutory provision; cf *N. Raschauer /Riesz*, art 8, recital 14 in Holoubek/Lienbacher (eds), Charter (2014).

54) In this respect, the access to personal data and their processing radius is limited and their period of use determined; cf *N. Raschauer /Riesz*, art 8, recital 14 in Holoubek/Lienbacher (eds), Charter (2014).

55) The consent exists basically by a non-verbal conduct within the meaning of art 863 of the Austrian Civil Code (ABGB), which can be granted also implicit. However, mere silence does not imply consent.

56) The wording of paragraph 2 is (obviously) deliberately drafted in an open way. It could be considered whether this should also enable a weighing of benefits in *inter privatos* relationships (eg current address of a debtor, credit information).

57) Here, this alternative is understood as a »general« statutory authorization, as the Charter refers, for example, to statutory tasks assignments in other laws.

58) It is to be assumed that art 8 para 2 of the Charter did not want to restrict the data processing authorization of the former Data Protection Directive 95/46/EC, which refers to the phrase »some other legitimate basis laid down by law«. These indefinite definitions of norms are more likely to be aimed at other cases of data processing not explicitly covered by art 8 para 2 of the Charter, provided that they have *at least* a legal basis and comply with the other requirements of art 8 para 2 of the Charter. Consequently, this permission shall be interpreted broadly.

59) ECJ 20. 5. 2003, C-465/00, *ORF*, ECLI:EU:C:2003:294 recital 74 f.

60) Or in the words of the GDPR: particularly worthy of protection (art 9 GDPR).

61) cf once again Selected Judgements of the Constitutional Court (VfSlg) 19.973/2015.

62) cf Selected Judgements of the Constitutional Court (VfSlg) 19.632/2012.

63) cf in detail, art 29 Working Party, Opinion 06/2014, 844/14/EN (to the Directive 95/46/EC).

64) Lit f shall not apply to the processing carried out by public authorities in the performance of their duties.

65) In our case, the person responsible within the meaning of art 4 no 7 GDPR is the parent company.

66) The purpose of the data processing does not have to be mentioned explicitly in the text, but may also arise due to the interpretation of the norm in individual cases *(Reimer*, art 6 recital 24 in Sydow (ed), GDPR [2017]).

67) *Reimer*, art 6 recital 22 in Sydow (ed), GDPR (2017).

68) *Reimer*, art 6 recital 54 in Sydow (ed), GDPR (2017).

69) *Reimer*, art 6 recital 57 in Sydow (ed), GDPR (2017).

70) Art 45 ff GDPR are not discussed in detail here, since they regulate the transfer of data from the EU to third countries, but not the transfer of data from third countries to the EU.

Meta-Daten

Schlagwort(e)

internal audit, group audit, audit rights.

Rubrik(en)

Aufsatz

Rechtsgebiet(e)

Finanzmarktrecht

Verweise

› § 39 BWG
› § 42 BWG
Art 11 RL 2013/36/EU
Art 74 RL 2013/36/EU
Art 109 RL 2013/36/EU
Art 6 VO (EU) 2016/679 (DSGVO)
Art 8 GRC