MEMORANDUM OF UNDERSTANDING

BETWEEN THE

UK FINANCIAL REPORTING COUNCIL AND THE

SWISS FEDERAL AUDIT OVERSIGHT AUTHORITY

ON COOPERATION RELATED TO THE OVERSIGHT OF AUDITORS

The Federal Audit Oversight Authority (FAOA), based on its obligations under the Swiss Federal Act of 16 December 2005 on the Licensing and Oversight of Auditors (Audit Oversight Act, AOA; SR 221.302) and the implementation of the legislation based thereon;

and

The Financial Reporting Council Limited (FRC), based on its obligations under the Companies Act 2006,

have agreed as follows:

PURPOSE

1. Both Parties seek to improve the quality, accuracy and reliability of the audit of public companies through audit regulation and auditor oversight so as to protect investors, help strengthen public trust in the audit process and increase investor confidence in their respective capital markets. Given the global nature of capital markets the Parties recognise that it is in their common interest to cooperate in the oversight of auditors that fall within the regulatory jurisdiction of both Parties, to the extent such cooperation is compatible with the Parties' respective laws or regulations, their important interests and their available resources. They also recognise the importance of cooperation to avoid an undue burden on audit firms of overlapping supervision.

2. The purpose of this MOU is to facilitate mutual cooperation between the Parties, to the extent permitted by their respective national laws, in the area of public oversight, registration, inspections and investigations of auditors of companies that are subject to the regulatory jurisdictions of both the FAOA and the FRC.

3. This agreement recognises that the European Commission has decided upon the equivalence referred to in Article 46, paragraph 1 of the Directive 2006/43/EC in respect of Switzerland.

4. This agreement recognises that the European Commission has decided upon the adequacy referred to in Article 47, paragraph 1(c) of the Directive 2006/43/EC in respect of Switzerland, enabling the exchange of audit working papers between the EU Member States' oversight authorities and Switzerland.

DEFINITIONS

5. For the purpose of this MOU,

"**Auditor**" means a natural person or an audit firm that is subject to the oversight of both Parties in accordance with the Companies Act 2006 and the Audit Oversight Act in Switzerland;

"**Information**" refers to public and non-public information and/or documents that include but are not limited to: (1) reports on the outcome of inspections and investigations, including information on firm-wide procedures and engagement reviews, (2) audit working papers or other documents held by auditors, and (3) other areas of mutual interest for the purpose of supervision, provided that the information relates to matters that are subject to the regulatory jurisdictions of both Parties.

"**Inspections**" refers to external quality assurance reviews of auditors generally undertaken on a regular basis with the aim of enhancing audit quality.

"**Investigations**" refers to investigations in response to a specific suspicion of infringement or violation of laws or regulations.

"**Laws or regulations**" mean any laws, rules or regulations in force in the respective countries of the Parties;

"**Party**" or "**Parties**" means the Federal Audit Oversight Authority in Switzerland and/or the Financial Reporting Council in the UK;

COOPERATION

Mutual recognition

6. The Parties will rely on the supervision of the auditors in their home country and shall in general refrain from public oversight activities, inspections, investigations and penalties with respect to auditors from the other country on the basis of reciprocity, to the extent permitted by their respective laws or regulations.

7. The Parties will endeavour to minimise the burden related to the registration of auditors from the other country on the basis of reciprocity, to the extent permitted by their respective laws or regulations.

8. The Parties will use their best endeavours to inform one another, prior to or immediately after taking any significant public oversight measures in respect of relevant auditors that are registered or seek registration in the other country, to the extent permitted or required by laws or regulations.

9. In exceptional circumstances, cooperation may include one Party assisting the other Party in an inspection or an investigation by performing activities that may include but are not limited to facilitating access to information and/or, if requested, reviewing audit work papers and other documents.

Exchange of information

10. Cooperation includes the exchange of information between the Parties for the purposes of facilitating cooperation in the areas of public oversight, registration, inspections, and investigations of auditors, to the extent permitted or required by laws or regulations.

Requests for Information

11. Requests will be made in writing (including e-mail) and addressed to the contact person of the requested Party.

12. The requesting Party should specify the following:

    a) the information requested;

    b) the purposes for which the information will be used;

    c) the reasons why the information is needed, and if applicable, the respective laws or regulations that may have been violated;

    d) an indication of the date by which the information is needed; and

    e) an indication, to the best of the knowledge of the requesting Party, whether the information requested might be subject to further use, disclosure or transfer under paragraphs 26 to 29.

13. Any request for information which is held exclusively by the relevant auditor shall be made to the other Party and not directly to the relevant auditor.

14. In cases where the information requested may be maintained or available at another authority within the country of the requested Party, the requested Party will endeavour to provide the information to the extent permitted by laws or regulations.

Execution of requests for Information

15. Each Party will provide the other Party with information upon request, subject to paragraph 19 below.

16. Each request will be assessed on a case by case basis by the requested Party to determine whether information can be provided under the terms of this MOU. In any case where the request cannot be met in full within the desired time period, the requested Party will inform the requesting Party accordingly, and will consider whether other relevant information or assistance can be given.

17. Each Party will endeavour to provide a prompt and adequate response to requests for information.

18. In order to avoid unnecessary delays, the requested Party will provide, as appropriate, parts of the requested information as they become available.

19. The requested Party may refuse to act on a request where:

    (a) it concludes that the request is not in accordance with this MOU;

    (b) acceding to the request would contravene the laws or regulations of the requested Party's country, in particular if the information is to be passed on to criminal prosecution authorities or to authorities and bodies with powers to impose sanctions under administrative law and, due to the nature of the offence, legal assistance in criminal matters would be excluded.

    (c) it would burden the requested Party disproportionately;

    (d) it concludes that it would be contrary to the public interest of the requested Party's country for assistance to be given;

    (e) the provision of information would adversely affect the sovereignty, security or public order of the requested Party's country; or

(f) judicial proceedings (civil, criminal or administrative proceedings) have already been initiated, or have become legally effective, in respect of the same actions and against the same persons before the authorities of the country of the requested Party.

20. The requested Party will promptly inform the requesting Party of the reasons, where it refuses to act on a request made under this MOU.

21. Any document or other material provided in response to a request under this MOU, and any copies thereof, shall be returned on request to the extent permitted by laws or regulations.

CONFIDENTIALITY

22. Each Party shall keep confidential all information received or created in the course of cooperation in accordance with the terms of this MOU, subject to paragraphs 26 to 29. The obligation of confidentiality shall apply to all persons who are or have been:

    (a) employed by the Parties;

    (b) involved in the governance of the Parties; or

    (c) otherwise associated with the Parties.

23. The Parties have established and will maintain such safeguards as are necessary and appropriate to protect the confidentiality of the information, including storing the information in a secure location when not in use.

24. The Parties have provided each other a description of their applicable information systems and controls and a description of their laws and regulations that establish appropriate limits on access to non-public information.

25. The Parties will inform each other if the safeguards, information systems, controls, laws or regulations referred to in paragraphs 23 and 24 above change in a way that weaken the confidentiality of the information and/or documents provided by the other Party.

USE OF INFORMATION

26. The Parties may use information received or created in the course of cooperation only for the exercise of their functions of public oversight, inspections and investigations of auditors. If either Party intends to use information received or created in the course of cooperation for any purpose other than those stated in the request (including by

transferring the information internally) it must obtain the prior written and specific consent of the requested Party. If the requested Party consents to the use of information for a purpose other than that stated, it may subject such use to conditions.

EXCEPTIONS TO CONFIDENTIALITY

27. In the event that the requesting Party is required to disclose or to transfer information received or created in order to comply with its obligation under its laws or regulations or by a court order, it will provide, wherever possible, at least fifteen working days written notice to the requested Party prior to the disclosure or transfer, stating why it is required to disclose or to transfer the information.

28. If the requested Party objects to the disclosure or transfer of information received or created, the requesting Party will make its best efforts to resist the disclosure or transfer of the information received or created.

29. A Party that intends to disclose or to transfer to a third party information received or created, other than in cases referred to in paragraph 27, must obtain the prior written and specific consent of the Party which provided the information. The Party which intends to disclose or to transfer the information shall give the reasons and the purposes for which it would be disclosed or transferred. The requested Party may make its consent to the disclosure or transfer of the information subject to conditions.

THE TRANSFER OF PERSONAL DATA

30. The Parties will only transfer personal data in accordance with their respective laws or regulations on data protection.

OTHER

31. This MOU does not create any binding legal obligations, nor does it modify or supersede any laws or regulations in the UK or in Switzerland. This MOU does not give rise to a right on the part of the FRC, the FAOA or any other governmental or non-governmental entity or any private person to challenge, directly or indirectly, the degree or manner of cooperation by the FRC or the FAOA.

32. This MOU does not prohibit the Parties from taking measures with regard to the supervision of auditors that are different from or in addition to the measures set forth in this MOU.

33. The Parties shall at the request of either Party consult on issues related to the matters covered by this MOU, and otherwise exchange views and share experiences and knowledge gained in the discharge of their respective duties to the extent permitted by their respective laws or regulations.

34. The Parties may consult informally, at any time, about a request or proposed request or about any information provided.

35. The Parties may consult and revise the terms of this MOU in the event of a substantial change in laws or regulations and/or practices affecting the operation of this MOU, or if they wish to modify the terms of their cooperation.

ENTRY INTO EFFECT AND TERMINATION

36. This MOU will come into force from the date of signature by both Parties.

37. This MOU may be terminated by either Party at any time. The provisions concerning confidentiality (paragraphs 22 to 29) and on the transfer of personal data (paragraph 30) shall remain in force thereafter.

For the Federal Audit Oversight Authority

Thomas Rufer
(Chairman of the Board of Directors)
Date: 18. März 2014

Frank Schneider
(Chief Executive Officer)
Date: 18. März 2014

For the Financial Reporting Council

Paul George
(Executive Director, Conduct and FRC Board Member)
Date: 6 MARCH 2014

FRC CONFIDENTIALITY AND INFORMATION SECURITY POLICY AND PRACTICES

1. Laws and Regulations Relevant to Access to Information Held by the Financial Reporting Council

Legal Restrictions on Disclosure

1.1. The Companies Act 2006 imposes restrictions on the disclosure of information that relates to the private affairs of an individual or to any particular business that is provided to the Financial Reporting Council (as the designated body for the purposes of section 1252[1]), in connection with its statutory functions for the regulation of statutory auditors, or to the Audit Quality Review team (AQR), as the independent monitoring body.

1.2. Specifically, Section 1224A(3) prohibits the disclosure of any such information not already available to the public without the consent of the individual or person responsible for the business. Sections 1224A(4) and (5) set out the exceptions to that prohibition, that enable the FRC to disclose information it has received in the following cases:

- disclosures to enable the FRC to carry out the functions in Part 42 of the Companies Act 2006. The principal functions are the recognition and oversight, in accordance with the statutory requirements, of accountancy bodies (i) known as Recognised Qualifying Bodies, that offer an audit qualification and/or (ii) known as Recognised Supervisory Bodies, that supervise statutory auditors.

- disclosures made to a person specified in Part 1 of Schedule 11A, a copy of which is attached hereto. This lists a number of public authorities and regulatory bodies as specified persons

- disclosures made for a purpose specified in Part 2 of Schedule 11A, a copy of which is attached hereto. This lists a number of purposes related in the vast majority of cases to statutory regulatory functions

- disclosures to a competent authority in the European Economic Area responsible for the regulation or oversight of auditors, in accordance with Section 1253B; and disclosures to a competent authority in a third country responsible for the regulation or oversight of auditors, in the case of audit working papers, in accordance with specific statutory provisions (see 1.4 to 1.6 below) and, otherwise, for the purposes of enabling that authority to exercise its functions.

1.3. A disclosure made in contravention of these requirements is a criminal offence under section 1224B, with penalties of imprisonment or a fine. Section 1224B provides a defence to the offence where the person did not know and had no reason to suspect that the disclosure had been made, or where the person took all reasonable steps and exercised due diligence to avoid the commission of the offence.

---

[1] The Secretary of State has delegated most of his responsibilities for audit regulation through the Statutory Auditors (Amendment of Companies Act 2006 and Delegation of Functions etc) Order 2012 Order 2012 (SI 2012/1741)

Specific Statutory Provisions in relation to audit working papers

1.4. Section 1253E includes additional restrictions on the disclosure of audit working papers obtained from a third country competent authority or a third country audit firm:

- Section 1253E(3) requires that any working arrangements with third countries must provide that the FRC may not use audit working papers obtained other than in connect with audit regulation (quality assurance, investigation and discipline, public oversight).

- Section 1253E(5) requires that the FRC and persons employed or formerly employed in discharging its statutory functions must be subject to "obligations of confidentiality as to personal data, professional secrets and sensitive commercial information contained in audit working papers transferred [to the FRC]".

Common Law Duty of Confidentiality

1.5. Under common law, that is law applied by the courts by reference to previous cases, the general position in the UK is that, if information is given in circumstances where the recipient owes a duty of confidence or where the information is by its nature "confidential", then that information cannot normally be disclosed without the information provider's consent. There are some circumstances where disclosing otherwise confidential information is lawful, in particular:

- where disclosure is in the overriding public interest;
- where there is a legal duty to do so, for example a court order.

Ability of the FRC to Transfer Confidential Information to Other Entities.

1.6. The legal framework that permits the FRC to transfer otherwise confidential information to other bodies or for specified purposes is set out at 1.2 above. Although there is no statutory provision that only permits transfers where the recipient itself has specified confidentiality arrangements in place, since transfers are permitted only to specified bodies carrying out public interest functions or for specified regulatory functions, there is an expectation that adequate confidentiality arrangements will be in place in the recipient body.

Freedom of Information Act

1.7. The FRC is subject to the Freedom of Information Act 2000 (FOIA) which provides public access to information held by public authorities on the principle that people have a right to know about the activities of public authorities. The FRC is a public authority for part of its functions; its statutory duties delegated to it by the Secretary of State which includes the registration of third country auditors. The right of access is subject to a number of exemptions and we would consider the application of the exemptions to any requests in relation to information provided by a foreign authority in the course of providing international assistance. The exemptions likely to apply would include Section 41 which states that information will be exempt if it was obtained from another person or organisation and disclosure would result in a breach of confidence over which a person could take legal action and Section 44(1) (a) which provides for the exemption of information where its disclosure is prohibited by other legislation. Provisions in existing legislation prohibiting the disclosure of information are referred to as statutory prohibitions or statutory bars and require a public authority not to disclose specific information.

Data Protection

The Data Protection Act 1998 provides for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. Any personal data provided to the FRC must be processed in accordance with the principles set out in the Data Protection Act. Further, section 1224A, subsection (7) makes it clear that the requirements of the Data Protection Act 1998 apply to the disclosure of information by the FRC.

Decision to Transfer Confidential Information

1.8. A decision to transfer confidential information held by the FRC to another person is taken on the merits of the individual case within the legal framework set out above. Any such decision must be made with the approval of the Chair, Conduct Committee and the Executive Director, Conduct Division (the Conduct Division is a part of the FRC), other than in exceptional circumstances.

2. Obligations on Staff and Board members for the maintenance of the confidentiality of non-public information

2.1. The statutory and common law obligations in respect of information disclosure are supplemented by Codes of Conduct and requirements that apply to staff of the FRC and the AQR, and to members of the FRC and its Conduct Committee.

Board Members

2.2. The FRC has a Code of Conduct for all non-executive and executive members of the Board of FRC Ltd and all members of the sub committees of the FRC and this therefore applies to all members of the Conduct Committee and governs the conduct of their work as a Board member. The Code sets out general principles and covers the collective and individual responsibilities of Board Members, conflicts of interest, hospitality and gifts, and confidentiality.

2.3. On the confidentiality of information, the Code states:

All information acquired by Board members in the exercise of their functions as Board members during their appointment is confidential to the FRC and/or its Committees. Board members must not during their appointment or afterwards (unless he or she is authorised by the FRC Chair or the relevant Committees or is under a legal obligation to do so):

i. use for his/her own benefit or the benefit of any other person; or
ii. disclose to any person; or
iii. through any failure to exercise all due care and diligence, cause or permit any unauthorised disclosure of:
any confidential information that he or she obtains by virtue of their position as a Board member.

In addition, there is a specific responsibility on Board Members that they must not misuse information gained in the course of their service for personal gain.

2.4. The most likely sanction against a breach of confidentiality by a Board member is removal from the Board following due consideration by the FRC Nominations Committee. In addition a Board Member may have committed a criminal offence under section 1224B (see above).

Staff and former Staff

2.5. There are similar obligations on staff of the Financial Reporting Council, including AQR staff that they must keep confidential all unpublished information they acquire through their role at the FRC, unless the disclosure of that information has been properly authorised.

2.6. A member of staff in breach of the confidentiality requirements in their employment contract would be subject to the FRC's Disciplinary Procedures. The confidentiality provisions continue to apply following the end of employment and we would consider taking legal action in response to a breach by a former member of staff. In addition, they may have committed a criminal offence under section 1224B (see above).

3. Information Systems and Controls Relating to the Security of Information

3.1. The Conduct Division and the FRC attach great importance to systems and practices designed to protect the confidentiality, integrity and availability of the confidential information that is held. These arrangements cover both the security of physical documents and information held in electronic form and are intended to meet the UK's Seventh Principle of Data Protection; that the measures employed ensure a level of security appropriate to the nature of the data to be protected and the harm that might result from any unauthorised or unlawful processing, as well as accidental loss or destruction or damage to any personal data.

Protecting Physical Documents in the FRC Offices

3.2. The FRC offices are located on a single floor of an office building, which has security guards at the entrance and security patrols that operate throughout the building outside office hours, seven days a week. The FRC offices have restricted access with card access readers on the perimeter doors and a further reader on the door that separates meeting rooms from the offices themselves. The FRC requires that all staff have picture identification badges. Visitors to the FRC must wear temporary identification badges and are escorted at all times within the office area.

The FRC facilities are also protected by fire detection, alarming and suppression systems.

3.3. Any documents provided by the FAOA to the FRC in accordance with the Memorandum of Understanding will be kept in a locked cabinet when not in use. Confidential physical documents that are no longer required are disposed of in locked bins for shredding and secure disposal.

Protecting Physical Documents away from the FRC Offices.

3.4. FRC staff may only take confidential documents out of the FRC offices when necessary and are reminded that they need to take great care to protect both the physical document and the content.

3.5. Protecting confidential information away from the FRC offices is of particular importance for staff of the AQR, whose work is largely conducted at the major audit firms, who are responsible for providing secure accommodation and storage facilities for IT equipment and documents.

Protection of Confidential Electronic Information

3.6. All members of staff are bound to follow the FRC IT Security policy, which forms part of their terms and conditions of employment. All Managers monitor their staff and report any IT Security concerns to the Head of IT. The FRC outsources the running of a fully managed IT service on its behalf and any suspicious matters are escalated to the Head of IT. Information held electronically is protected by a system of passwords which governs all network access accounts and enforces password complexity and change frequency requirements. Each individual authorised to access information and documents has a unique user name and password. This username and password combination is required to authenticate the individual requesting information to the computer, application or network environment providing the information. User names are generally not private information whereas the password must be held in strict confidence by each individual. The arrangements dictate the minimum length, complexity and length of validity of a password, enforced through technical controls at the application and operating system levels.

3.7. Passwords do not provide access to all levels of the system. A system of access control grants access to employees through the line management chain of command as is necessary to enable the individual to do his or her job. All access permissions are promptly revoked when an individual ceases to be an employee or contractor. All Passwords are changed every 30 days and complex passwords are in use. If a password is not changed, then network access is withdrawn until the password is changed. All users are locked out of the network after three failed attempts.

3.8. All users have the ability to create 256bit encrypted zip files to protect individual files or folders so that they remain secure when they are emailed or carried on removable media. The AQR uses a separate proprietary electronic audit management system that maintains all the work programmes and documentation relating to audit inspection. The system cannot be accessed by staff from other units within the FRC and is subject to separate password controls.

3.9. Electronic information is further protected by a screen-saver policy, such that all FRC computers activate a screen-saver after 30 minutes of inactivity, which then requires the user's password to be re-entered in order to continue.

3.10. The FRC server room within the office has separate tightly restricted access, which is reviewed regularly. All of the computer systems are protected by UPS and alerting has been setup to inform the Service desk of any power related issues. The Server Room is air-conditioned and has N+1 resilience and would cope with a single AC unit failure. All FRC data is backed up daily and Backup tapes are removed off site twice a week and are password protected. All remaining tapes are stored in a locked cupboard on-site. The FRC is currently reviewing a cloud based solution. The solution is approved to Impact Level (IL2). The Impact Levels are defined by the Cabinet Office and the National Technical Authority for Information Assurance for UK Government. The solution has an up time of 99% and is approved for use by Governmental departments.

3.11. The system also provides for the generation of a security audit trail that contains information to enable the investigation of a loss of data or improper access to data. In particular, the system associates user identification information with any system request or

activity, so that the initiating user can be held accountable for that request or activity. Audit logs are enabled at the operating system. Individual account identifications are tied to the operating system to ensure proper accountability. Network access activity logs are maintained and reviewed regularly for inappropriate access.

3.12. In addition, all IT assets (for example desktop and laptop computers, computer files, electronic mail) are the property of the FRC and subject therefore to specific controls. For example, these prevent the installation of unauthorised software on any FRC computer and ensure that all data held on laptops that are used outside the FRC offices include a high level of encryption for all data. All handheld devices and laptops are encrypted and all users are forced to change the encryption passwords every 30 days.

3.13. All applications and operating systems have security flaws and the FRC has a policy of applying security patches in a timely manner to applications and operating systems, as these flaws are identified. This helps to ensure that applications and operating systems are protected from the threat of hacking, cracking and malware attacks by repairing any known security flaws. Regular monthly patching of the Server and Desktop/Laptop estate takes place as part of the managed service by the service provider. In terms of email exchange this is captured by the Websense service. All IT Security breaches are reported to the Head of IT who will then take any necessary action. The patch management process is initiated on a monthly basis and incorporates the following steps:

- Identification of patches to be applied
- Evaluation of risk and establishment of patch priority
- Patch testing
- Patch deployment

3.14. The FRC also uses software tools such as Intrusion Prevention systems (IPS), firewalls and anti-virus system software to protect its IT resources from malicious access. All emails are scanned and cleaned externally before they are delivered to the FRC infrastructure which means no virus enter the FRC Network.

3.15. FRC staff must take appropriate steps to limit the risk of the introduction of malicious code. In particular, they are prohibited from disabling any anti-virus software and must always follow proper policy and procedures when downloading and installing files or software on any IT assets in their custody. A staff member who fails to follow these requirements and whose conduct disrupts the normal operation of the FRC's IT systems is liable to disciplinary action, which includes the possible termination of employment.

3.16. To access the FRC Network remotely, all users require a User name, their network password, Pin details and a number generating security token. If any one of these factors is incorrect, then the user will not gain access to the Network.

3.17. SSL technology is used by the FRC to safeguard the data that is held on its website. We do not store any confidential data on the website and our internal systems are protected by multiple layers of authentication when they are accessed remotely. We do not currently have a regular programme of risk/vulnerability assessments, as there is very little change to our infrastructure and we believe the regular patching deals with all threats. We are planning to carry out a risk assessment in 2014, once we have moved to the new solutions.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Audit Oversight Authority FAOA

Privileged and confidential

Date: 1st September 2012
To: Foreign Audit Oversight Authorities (MOU)

Description of FAOA laws and regulations that establish appropriate limits on access to non-public information and/or documents

The purpose of this memo is to provide a summary overview of the laws and regulations that establish appropriate limits on access to non-public information and/or documents within the FAOA.

a) Scope of the official secrecy and confidentiality rules

The bodies of the FAOA and its personnel are bound by official secrecy (Art. 34 Audit Oversight Act; AOA; SR. 221.302)[1]. The breach of the secrecy is a criminal offence (cf. Art. 320 Swiss Criminal Code; SR 311)[2]: Whoever reveals a secret that was entrusted to him in his capacity as a member of an authority or as an official, or of which he learned due to his official position or employment, shall be punished with imprisonment for up to three years or a monetary penalty. The violation of the official secret shall also be liable to punishment following termination of the official position or employment relationship.

The FAOA can for the purpose of execution of its responsibilities call upon the services of third parties. These parties are also legally bound to preserve the secrecy about all matters of which they become aware in performing their work (Art. 20 AOA). The breach of this secrecy is also a criminal offence (cf. Art. 40, para. 1, letter d AOA): Imprisonment of up to three years or a pecuniary penalty of up to 1,080,000 Swiss francs is imposed on whoever during or after completion of an activity as a third party engaged by the FAOA, discloses a secret that has been entrusted to the person in this capacity or the person has come aware of in this capacity; federal provisions on the duty to testify and the duty to inform an authority remain reserved.

Further to these legal prescriptions, the FAOA enacted a Code of Ethics for the FAOA staff, which sets out the principles for the code of conduct, conditions and situations of

[1] http://www.revisionsaufsichtsbehoerde.ch/bausteine.net/file/showfile.aspx?downdaid=7628&sp=D&domid=1063&fd=2

[2] http://www.admin.ch/ch/e/rs/3/311.0.en.pdf

Federal Audit Oversight Authority FAOA
P.O. Box 6023
CH-3001 Berne
Switzerland
phone: +41 31 560 22 10; fax +41 31 560 22 23
e-mail: info@rab-asr.ch
www.audit-oversight.ch

incompatibility in the course and after employment with the FAOA, and administrative sanctions imposed in the event of any infringement. The Code of Ethics is applicable to all employees of the FAOA (Art. 1 Code of Ethics). Article 15 of the Code of Ethics FAOA states again the principle of the official secrecy according to Article 34 AOA and specifies that FAOA staff is allowed to testify as a party, an expert or a testimony in a matter which relates to the FAOA only after the consent of the FAOA Board. The FAOA Board as well as all FAOA employees have to confirm annually and in writing that they have read and understood the Code of Ethics and will comply with all the rules set out in the Code.

b) Publication of information

Rules and regulations with regard to publication of confidential information are very restrictive in Switzerland. FAOA inspection reports and investigations are non-public information. Under Article 19 Paragraph 2 AOA, the FAOA is required to provide information to the public about ongoing and closed proceedings where necessary for prevailing reasons of public or private interest. Under this rule, the FAOA would for instance take action to rectify misleading wrong information broadcasted in the media. To this day, there has been no incident where the FAOA has actually applied Article 19 Paragraph 2 AOA.

c) Onward sharing of information

As a principle, non-public information is confidential information protected by the official secrecy. Transmission of confidential information to third authorities or parties is only possible if there is a legal basis for such a transmission. The AOA foresees the following possibilities of administrative or legal assistance:

- Oversight authorities under special law[3]: According to Article 22 AOA, the FAOA and the oversight authorities under special laws must provide one another with all the information and forward the documents that they require for the enforcement of the applicable legislation. They inform each other about pending proceedings and decisions that could be relevant for their respective oversight activities.
- Stock exchange: According to Article 23 Paragraph 2 AOA, the FAOA and the stock exchange inform each other about pending proceedings and decisions that could be relevant for their respective oversight activities.
- Criminal prosecution authorities: According to Article 24 AOA, the FAOA and the criminal prosecution authorities must provide one another with all the information and forward documents that they require for the enforcement of the AOA. The criminal prosecution authority may use the information and documents received from the oversight authority only for the purpose of the criminal proceedings, for which legal assistance was granted. It may not pass on the information and documents to third parties.
- Federal Council (Government) and Federal Assembly (Parliament): The FAOA is subject to the oversight by the Federal Council (Art. 38 AOA). It annually submits a report on its

[3] The law still reads "oversight authorities under special laws" because until 31 December 2008, government supervision of banks (SFBC), insurance undertakings (FOPI), and other financial intermediaries were entrusted to separate oversight entities. As of 1 January 2009, these oversight authorities were consolidated into a single Swiss Financial Market Supervisory Authority (FINMA). For that reason, this rule applies in principle only to the FINMA.

activities to the Federal Council and to the Federal Assembly. Generally, the Federal Council or the Federal Assembly would not ask for any documents other than the annual FAOA activity report, which is not confidential. It can however not be excluded that under certain circumstances, the Federal Council or the Federal Assembly may ask for more detailed information on a specific file.

These rules allow the FAOA in principle to forward confidential information to the national bodies stated above[4]. The FAOA takes however the view that the aforementioned provisions only apply to information and documents received from national sources or created by the FAOA itself. Should a Swiss court or authority solicit information or documents provided by a foreign authority, the FAOA would only approve of the request, if deemed appropriate, with the prior consent of the foreign authority in accordance with the memorandum of understanding concluded with it.

All Swiss oversight bodies to which information might be transferred by the FAOA carry out oversight duties that are in the public interest and are bound by official secrecy rules. This means that receiving entities are not able to transfer the information received on to a third party without first requesting consent from the FAOA (which, in turn, would seek the consent by the foreign authority). The breach of the secrecy by any of these Swiss oversight bodies is a criminal offence (cf. Art. 320 Swiss Criminal Code). Further to the general rules, the following specific rules might be of interest with regard to confidentiality:

- FINMA: According to Article 14 Financial Market Supervision Act (FINMASA; SR 956.1)[5], the organs, the staff and the management bodies of the FINMA must observe secrecy on official matters. The duty of secrecy continues to apply after termination of employment or membership of a management body of FINMA. The staff and the individual members of the management bodies of FINMA may not without authorization from FINMA disclose in evidentiary hearings and in court proceedings as parties, witnesses or expert witnesses matters that have come to their knowledge in the course of their duties and that relate to their official tasks. Furthermore, official secrecy applies to all mandatories of FINMA (investigating agents, restructuring agents, liquidators, administrators in bankruptcy and other mandatories).
- Stock exchange: The bodies of the Swiss Stock Exchange and its personnel are bound by professional secrecy rules. According to Article 43 of the Stock Exchange Act (SESTA; SR 954.1)[6], whoever intentionally discloses a secret which has been confided to him in his capacity as an organ, employee, mandatory or liquidator of a stock exchange or a securities dealer, as an organ or employee of an auditing company, or of which he has become aware in any such capacity and whosever intentionally attempts such breach of professional secrecy by inducement shall be punished by imprisonment of up to three years or pecuniary penalty. The duty of secrecy continues to apply after termination of employment or membership of a management body. The cantons (federal states) shall be responsible for the prosecution and adjudication of any breaches of this provision. The general provisions of the Swiss Criminal Code shall apply.

---

4 There is no provision on legal assistance by FAOA to civil courts in the Audit Oversight Act, which can be interpreted as a prohibition. Even if there is no prohibition, civil process orders would not enable a civil court to order the FAOA to provide confidential information. Legal assistance would be only possible with the consent of FAOA.

5 http://www.admin.ch/ch/e/rs/9/956.1.en.pdf

6 http://www.six-exchange-regulation.com/download/admission/regulation/federal_acts/sesta_en.pdf

- Criminal prosecution bodies: Based on Article 320 Swiss Criminal Code, all cantonal criminal prosecution bodies are bound by official secrecy. Any breach of that secrecy is a criminal offence. All 26 cantonal organizational laws contain implementation regulations of the official secrecy.
- Federal Council and Federal Assembly: The members of the Federal Council and of the Federal Assembly are bound by official secrecy. With regard to the members of the Federal Assembly, any breach of that secrecy is a criminal offence (Art. 8 Federal Act on the Federal Assembly [Parliament Act, SR 171.10])[7].

d) Rules applying to the protection of personal data

The protection of personal data is governed by the Federal Act on Data Protection (DPA, SR 235.1)[8]. The DPA provides an overall framework and deals with data protection using principles similar to those applied in other countries. The Act extends the protection of private persons provided by the Swiss Civil Code (SCC; SR 210)[9] and regulates in a more detailed manner the processing of data by Federal authorities. The purpose of the DPA is to protect the privacy, interests and fundamental rights of data subjects. Furthermore, it has as its central goal the maintenance of good data file practice and the facilitation of international data exchange by providing a comparable level of protection.

The DPA is very wide in its scope and applies to personal data file activities carried out by Federal authorities, private organizations and individual private persons (excluding those for normal private purposes).

Switzerland is considered as providing an adequate level of protection for personal data transferred from the European Community (Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, 2000/518/EC notified under document number C(2000) 2304)[10].

The FAOA is also subject to the Federal Act on Freedom of Information in the Administration (FoIA, SR 152.3)[11]. This Act seeks to promote transparency with regard to the mandate, organisation and activities of the Administration (including bodies outside the Federal Administration, such as the FAOA). It aims at informing the public by ensuring access to official documents. This Act does not apply to official documents relating to international mutual and administrative assistance proceedings (art. 3, para. 1, letter a, nbr. 3, FoIA). Furthermore, the right of access shall be limited, deferred or refused if such access to an official document is likely to reveal professional, business or manufacturing secrets (art. 7, para 1, letter g FoIA). Based on the scope of application of the Act and the exceptions foreseen, the FAOA would not give access to documents provided in the course of international assistance by a foreign authority.

* * * * * * *

---

7 http://www.admin.ch/ch/e/rs/1/171.10.en.pdf

8 http://www.admin.ch/ch/e/rs/2/235.1.en.pdf

9 http://www.admin.ch/ch/e/rs/2/210.en.pdf

10 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0001:0003:EN:PDF

11 http://www.admin.ch/ch/e/rs/1/152.3.en.pdf