NOTE ON DATA PROTECTION IN THE FINANCIAL SECTOR

1. INTRODUCTION

In Liechtenstein the General Data Protection Regulation (Regulation EU/2016/679; GDPR) is generally directly applicable. As Liechtenstein is a member of the European Economic Area (EEA) and not the European Union, even European Regulations have to be incorporated into the EEA Agreement separately. On July 06, 2018, the EEA Joint Committee decided to incorporate the GDPR into the EEA Agreement (Decision of the EEA Joint Committee No 154/2018; OJ L 183, 19.7.2018, p. 23).
The GDPR thus entered into force for the EEA States Liechtenstein, Norway and Iceland on July 20, 2018 and has been directly applicable in Liechtenstein from that date.

Due to the incorporation of the GDPR into the EEA Agreement the Liechtenstein Data Protection Act (Datenschutzgesetz) as well as the Liechtenstein Data Protection Ordinance (Datenschutzverordnung) were completely revised in order to comply with Union Law and specify the applicability of enabling clauses provided by the European legislator.

However, there is not a specific regulation concerning data protection on the financial market in place in Liechtenstein. Instead, any processing of personal data of a data subject falls under the scope of the GDPR as well as the Liechtenstein Data Protection Act. There are no particular provisions regarding data protection in connection with financial regulation present in Liechtenstein.
European legislation on financial services also stipulates provisions on data protection of customers which have been implemented into national Liechtenstein law. The respective national acts for financial institutions and financial intermediaries (e.g. the Banking Act, Payment Service Act, Consumer Protection Act, UCITS Act, etc) refer to the Liechtenstein Data Protection Act and the GDPR respectively when it comes to provisions on data protection. These are the central regulations for all matters concerning data protection.

1.1. LEGISLATION

The following EU legislation, among others, is applicable:

- the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') is applicable to financial services with regard to their personal data processing activities.
- the Fourth Anti-money Laundering Directive (Directive (EU) 2015/849) as incorporated by Decision of the EEA Join Committee (Decision No 249/2018)
- the Payment Services Directive (Directive (EU) 2015/2366) ('PSD2'; entry into force of Joint Committee Decision is still pending. Therefore, PSD2 is not directly applicable in Liechtenstein. However, PSD2 has been implemented in Liechtenstein on a national level in the Payment Service Act or 'PSA'. As a consequence, recitals, interpretations of and guidelines concerning PSD2 are also relevant for Liechtenstein pursuant to established practice of Liechtenstein authorities.)

The European Data Protection Board ('EDPB') has issued the following Opinion:

- Opinion 4/2019 on the draft Administrative Arrangement for the transfer of personal data between the European Economic Area ('EEA') Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities

The Article 29 Working Party has issued the following guidance:

- Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing
- Letter of the Chair of the Article 29 Working Party to FATCA
- Letter regarding the PSD2 Directive

The European Banking Authority ('EBA') has issued, among others, the following guidance:

- Recommendations on Outsourcing to Cloud Service Providers (20 December 2017)
- Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2) (27 July 2017)
- Guidelines on Reporting Requirements for Fraud Data under Article 96(6) PSD2

The EC Directive on Privacy and Electronic Communication (2002/58/EC) as incorporated by Decision of the EEA Join Committee (Decision No 80/2003; OJ L 257, 9.10.2003, p. 31) is also applicable in Liechtenstein regarding the use of cookies and comparable technologies as well as the use of emails and marketing calls – that is until the mentioned Directive will be repealed by the proposed European ePrivacy Regulation (ePR).

EDPB Guidelines in general have to be taken into account when addressing questions on data protection in the financial services sector.

The following legislation of Liechtenstein, among others, is applicable (only available in German; German name in brackets):

- Data Protection Act ('DPA'; Datenschutzgesetz)
- Data Protection Ordinance ('DPO'; Datenschutzverordnung)
- Financial Market Authority Act ('FMAA'; Finanzmarktaufsichtsgesetz)
- Due Diligence Act ('DDA'; Sorgfaltspflichtgesetz)
- Due Diligence Ordinance ('DDO'; Sorgfaltspflichtverordnung)
- Banking Act ('BA'; Bankengesetz)
- Payment Service Act ('PSA'; Zahlungsdienstegesetz)
- Persons- and Companies Act ('PCA'; Personen- und Gesellschaftsrecht)

1.2. SUPERVISORY AUTHORITIES

The GDPR requires every Member State to establish a supervisory authority (Article 54 of the GDPR). In addition, the GDPR provides for a system of cooperation and transparency among all Member States' supervisory authorities in order to ensure consistent application of the GDPR throughout the EU.

The so-called 'Datenschutzstelle' (Data Protection Authority; https://www.datenschutzstelle.li/) is the supervisory authority for data protection in Liechtenstein pursuant to Article 54 of the GDPR.

As for the supervisory authority regulating the financial market, the Liechtenstein Financial Market Authority (FMA; https://www.fma-li.li/) is the competent national supervisory authority. The mandate of the Liechtenstein FMA for one includes the promotion of safety and soundness of banks, systemically important firms as well as other financial institutions and intermediaries and for another comprises of adhering to the integrity of the provision of financial services to customers and is responsible for fair treatment of consumers in the market as the authority on conduct and compliance matters. Pursuant to Article 4 of the Financial Market Authority Act ('FMAA') the FMA ensures the stability of the Liechtenstein financial market, the protection of clients, the prevention of abuses, and the implementation of and compliance with recognized international standards.
Pursuant to the mission statement of the Liechtenstein FMA the aim of regulation must always be to ensure that it is technological neutral, risk-based and non-discriminatory for existing market participants.[1]
The Liechtenstein FMA views data protection of customers as an essential concern and players on the financial market are responsible for securing customer data in compliance with the Data Protection Act and the GDPR and protecting it from fraud (cp. e.g. Article 64a of the Liechtenstein Banking Act which requires a notification system between the Liechtenstein

[1] https://www.fma-li.li/de/news/20170920-innovation-als-herausforderung-und-als-chance.html?comefrom=career

FMA and banking institutions as well as investment firms in order to submit notifications about data breaches among others).

2. PERSONAL AND FINANCIAL DATA MANAGEMENT

2.1. LEGAL BASIS FOR PROCESSING

Under the GDPR, personal data must be processed in accordance with the principles of fairness, lawfulness and transparency. In addition, processing shall only be lawful if (Article 6(1) of the GDPR):

- the data subject has given consent to the processing for one or more specific purpose;
- the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of a data subject prior to entering a contract;
- the processing is necessary for the compliance with a legal obligation to which the controller is subject;
- the processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- the processing is necessary to for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and
- the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

Moreover, under Article 9 of the GDPR, processing of special categories of personal data is prohibited unless one of the conditions in Article 9(2) applies.

Given that the abovementioned prerequisites for processing personal data are fulfilled - e.g. the processing of personal data is necessary for the performance under a contractual agreement or in order to fulfil duties imposed by law, or in order to comply with legitimate interests of the processor or a third party (i.e. due diligence or other compliance duties), the processing of data is in general allowed even if the data subject has not explicitly given consent to the processing for one or more specific purposes.

Article 4 (11) GDPR defines ‘consent’ of the data subject as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her, whereas recital 42 of the GDPR stipulates that Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.'

Regarding the element of 'freely given consent" the Article 29 Working Party ('WP29') Guidelines on Consent under the GDPR, notes that where an imbalance of power between the data subject and the data controller is present, it is unlikely that one may rely on consent for data processing. This is the case with relationships between an employee and employer or a public authority and an individual. In such cases consent to processing of personal data does not pose an appropriate lawful basis as it is regularly impossible to prove that consent was given freely.[2]
Institutions and intermediaries operating on the financial market therefore may not rely on the consent of a data subject for data processing unless the processing of data is fully optional as may be the case with marketing emails or newsletters.
Concerning financial market players, the data processing of a data subject is lawful if it is necessary for the compliance with a legal obligation. Such necessity is to be presumed with regard to required activities pursuant to European law such as the Anti-Money-Laundering-Directive (Know Your Customer; Anti-Money Laundering; Countering the Financing of Terrorism), PSD2 as well as the Markets in Financial Instruments Directive and Regulation (MiFID II, MiFIR) among others.

When a data controller is processing personal data, the data controller will be bound by a duty to inform the concerned data subject. The data subject in turn has the right to be informed in what manner, by whom and for how long their data is being processed.
In order to be compliant with the GDPR and the Data Protection Act it may be required to appoint a data protection officer who in turn may prepare internal data protection concepts as well as technical and organizational measurements for the respective company in order to comply with the right to be forgotten, the right to information, the right to data portability; notification procedures in case of a data breach etc).
Lastly, it may also be necessary to enter into data processing agreement with service providers with whom a data controller is undertaking business with (processor). In that regard it should be noted that it is not allowed to process data in countries which do not have the same level of data protection as is present within the EU or EEA. The assessment on whether the same level of data protection exists in a non-member-state may be derived from so-called adequacy decisions by the European Commission.

As for the lawfulness of data processing of a data subject for the purposes of the legitimate interests pursued by the controller or by a third party it should be noted that such lawfulness may not be assumed by all business interests in general which are oftentimes rather vague in nature. Pursuant to recital 47 of the GDPR the processing of personal data strictly necessary for the purposes of preventing fraud constitutes a legitimate interest of the data controller concerned.

[2] Article 29 Working Party Guidelines on consent under Regulation 2016/679 as last Revised and Adopted on 10 April 2018.

In general, data processing of financial institutions and financial intermediaries may be deemed legitimate when it concerns regulatory requirements which relate to unlawful acts in order to prevent fraudulent activities and terrorist financing.

2.2. PRIVACY NOTICES AND POLICIES

The GDPR establishes the principle of transparency (Article 5 of the GDPR). In addition, when data is being processed, information on the controller, purposes for processing, recipients of the data, retention period, and details of the data subject's rights shall be provided to the data subject (Article 13 of the GDPR).

The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used (recital 58 of the GDPR).

Financial institutions regularly specify the handling of data protection outside of the public privacy notices within their standardized or individual contractual agreements with other parties which must comply with the GDPR. As with other terms and conditions, terms on data protection must be received by the contracting party before the contract is concluded.

2.3. DATA SECURITY AND RISK MANAGEMENT

Taking into account the costs of implementation, nature, scope, context and purposes of processing, as well as the level of risk to the rights and freedoms of natural persons, data controllers and processors must implement technical and organisational measures to ensure a level of security appropriate to the risk (Article 32 of the GDPR).

In case processing of data is conducted through a data processor, a data controller must ensure that the data processing by the data processor complies with the regulations under the GDPR. In that regard Article 28 of the GDPR stipulates what contents need to be addressed in a contract between the data controller and the data processor such as subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller among other aspects.

While the security standards pursuant to the GDPR are not industry specific (e.g. for the financial services industry) a wide range of standards exists, which are valid globally like the Payment Card Industry Data Security Standards ('PCI DSS') and the Payment Application Data Security Standards ('PA DSS'). While both the Liechtenstein FMA and the Data Protection Authority have not commented on these certifications it goes without saying that a breach of these standards may also pose a violation of the duties under the GDPR respectively the financial market laws which refer to the GDPR.

PCI DSS is designed to implement mechanisms which protect card information during and after a financial transaction; PCI DSS was developed by the PCI Security Standards Council.

Additionally, pursuant to the Liechtenstein Persons- and Companies Act (in German 'Personen- und Gesellschaftsrecht'; PGR') the top-level management of a legal entity must manage and promote the undertaking of the entity with due care and is liable for observing the principles of careful management and representation. Consequently, the executive and potentially a supervisory board may become personally liable towards a legal entity if they do not implement sufficient data security and risk management policies and mechanisms which have to be adequate inter alia for the projected size of the undertaking and type of business which is conducted.

2.4. DATA RETENTION/RECORD KEEPING

Personal data must not be retained in a form which permits the identification of the data subject for longer than is necessary for the purposes the data was processed (Article 5(1)(e) of the GDPR). Moreover, the period for which the personal data are stored should be limited to a strict minimum, and to these ends, time limits should be established by the controller for erasure or a periodic review (Recital 39 of the GDPR).

Recital 50 of the GDPR states that a data controller may keep personal data for longer than the specified purpose, if the purpose of further processing lies in archiving purposes in the public interest of archiving, scientific or historical research purposes or statistical purposes. This exemption is generally unlikely to apply to financial institutions or intermediaries.
With regard to retention periods, there are no provisions stipulating that a concrete timeframe has to be defined concerning the record keeping. This is mostly due to the fact that such information on retention periods, if made public, may be abused by criminals.

3. FINANCIAL REPORTING AND MONEY LAUNDERING

Pursuant to the Liechtenstein Due Diligence regime the persons subject to due diligence must document compliance with the duties of due diligence and the duty of notification (e.g. notification to the Financial Intelligence Unit in case of money laundering) in accordance with the provisions of the Liechtenstein Due Diligence Act which implements the 4th Anti-money Laundering Directive and partially implements the 5th Anti-money Laundering Directive (Regulation EU/2018/843).

For this purpose, persons subject to due diligence must keep due diligence records and retain them. Customer-related documents, business correspondence and other proofs must be retained for ten years after termination of the business relationship or after an occasional transaction has been completed, whereas transaction-related documents, business correspondence and proofs must be retained for ten years after completion of the transaction

or after the business correspondence has been created (Article 20 of the Liechtenstein Due Diligence Act; 'DDA').

Subject to any legal provisions to the contrary, the persons subject to Art 20a DDA may process personal data, including special categories of personal data and personal data relating to criminal convictions and offences, exclusively for the purposes of preventing money laundering, organised crime and the financing of terrorism within the meaning of the Liechtenstein Penal Code and may not further process such data in a manner that is incompatible with the DDA. It is prohibited to process such data on the basis of the DDA for other purposes, such as commercial purposes.

4. BANKING SECRECY AND CONFIDENTIALITY

Liechtenstein enforces a rather strict banking secrecy/confidentiality. Pursuant to Art. 14 (1) Banking Act the members of the executive bodies of banks or investment firms as well as their employees and other persons working for such banks or investment firms are obliged to maintain secrecy with regard to facts which have been entrusted to them or made accessible to them on the basis of business relations with customers. The obligation to maintain secrecy applies indefinitely.

The statutory provisions on the obligation to testify and provide information to the criminal courts, supervisory bodies and the Financial Intelligence Unit ('FIU') as well as the provisions on cooperation with the FIU and with other supervisory authorities remain reserved.

Violations against the banking confidentiality is punishable by up to three years of imprisonment (Article 63 Banking Act).

Therefore, the possibilities for banking institutions and investment firms to disclosing information about their clients are very limited and closely related to criminal proceedings or AML/CFT regulation.

5. INSURANCE

Secrecy obligations in the insurance industry are similar to those of the banking industry. Pursuant to Art. 20 (1) of the Liechtenstein Insurance Distribution Act the members of the governing bodies of insurance intermediaries, reinsurance intermediaries and insurance intermediaries acting in an ancillary capacity and their employees and other persons working for such companies are obliged to maintain secrecy with regard to facts which are not publicly known and which have been entrusted or made accessible to them on the basis of business relations with customers. The obligation to maintain secrecy shall apply for an unlimited

period of time subject to the disclosure requirement in front of the criminal court as well as the FIU and other supervisory authorities.

Policyholders and other customers may release insurance intermediaries from the obligation of secrecy within the framework of the conclusion of the insurance contract or at a later date. The declaration to this effect must be made in writing and in full knowledge of the facts. In particular, the group of persons to whom the information may be disclosed must be clearly defined.

Infringements of this secrecy obligation is punishable by imprisonment of up to one year or a fine of up to 360 daily rates.

The protection of personal data must be in accordance with data protection legislation (GDPR and Data Protection Act).

6. PAYMENT SERVICES

Payment service Providers are governed by the Payment Service Act which is based on PSD2. Pursuant to Art. 100 PSA payment system operators and payment service providers are entitled to process personal data, including personal data relating to criminal convictions and offences, where this is necessary for the prevention, investigation and detection of payment fraud.

Payment service providers may process personal data only to the extent strictly necessary for the provision of their payment services and only with the consent of a payment service user.

Furthermore, the processing of personal data by payment service providers and the provision of information to natural and legal persons on the processing of their personal data is subject to data protection legislation.

When applying for a license as a payment service provider it is also necessary as part of the security control and risk mitigation measures to include Information on how a high level of technical security and data protection is ensured.

7. DATA TRANSFERS AND OUTSOURCING

See Chapter V of the GDPR for the general requirements regarding transfers of personal data to third countries or international organisations.

Transfer of personal data to third countries is restricted under the GDPR. However, transfers to countries for which an adequacy decision has been issued by the European Commission

are allowed. Thus far, the European Commission has recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protection.[3]

If the company receiving personal data from such a data transfer does not have its registered office in a country for which an adequacy decision has been issued, one of the safeguards pursuant to Art. 46 GDPR must be used.

In general, financial service providers have to notify the Liechtenstein FMA if they pursue to outsource key functions. Outsourcing of key functions is permitted, if

- neither the quality of the internal control nor the supervision by the FMA is significantly impaired;
- it does not lead to a delegation of the tasks of the management;
- the relationship and obligations of the financial service provider vis-à-vis its service users remain unchanged;
- the licensing requirements are not undermined; and
- none of the other conditions under which authorisation was granted are removed or altered.

Therefore, a financial service provider which outsources operational functions has to take reasonable steps to ensure that all legal requirements are still being complied with. The financial service providers remain responsible for the business areas which are being outsourced.

Banking institutions and investment firms in particular may outsource business areas at both nationally and internationally. However, The national and/or international outsourcing of data processing is only permitted if appropriate security measures are observed in the interest of protecting confidentiality and the customer is informed of the outsourcing when the data are transferred (Art. 14a BA).

These requirements are further specified in Art. 27g of the Liechtenstein Banking Ordinance. International outsourcing of data processing is only permitted if:

- the Liechtenstein and foreign regulations concerning bookkeeping, internal bank organisation, confidentiality and data protection are complied with;

[3] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

- all transactions are initiated in Liechtenstein and the client contact remains the sole responsibility of the Liechtenstein bank or investment firm;
- bookkeeping is kept in Liechtenstein and auditing is not made more difficult or restricted in any way;
- the audit office and the Liechtenstein FMA receive the necessary information from the competent foreign supervisory authority at any time regarding the regularity of data processing there;
- compliance with the above conditions is reported annually in a special section of the audit report and the lawfulness and regularity of data processing abroad is confirmed;
- cooperation between the Liechtenstein and foreign audit offices is ensured and the former have the possibility at any time to carry out audit procedures on site abroad;
- the competent foreign supervisory authority consents to this spin-off and confirms that the corresponding security arrangements meet its requirements;
- the foreign State concerned guarantees Liechtenstein banks or investment firms reciprocal rights for the processing of their data;
- customers are informed about data processing abroad.

Lastly, the Liechtenstein FMA may require the fulfilment of additional conditions

The EBA Guidelines on outsourcing arrangements[4] are also applicable and further specify the abovementioned requirements for outsourcing, such as making information available to regulators and understanding of the risks associated with outsourcing.

8. BREACH NOTIFICATION

As a general rule, it is mandatory for a data controller to notify the competent supervisory authority of any personal data breach (Article 33(1) of the GDPR).

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

In the case of a personal data breach, the controller is required to notify the Data Protection Authority without undue delay and, where feasible, not later than 72 hours after having

[4] EBA/GL/2019/02, https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1.

become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

For banking institutions, investment firms and insurance intermediaries the Liechtenstein FMA must have an effective and reliable reporting system in place with which potential or actual violations of the respective Acts and the regulations issued in connection therewith can be reported via a generally accessible, secure reporting channel. The reporting system has to include at least the protection of personal data in accordance with the Data Protection Act, both for the person reporting the breach and for the natural person claimed to be responsible for the breach.

With regard to payment service providers immediate notification of the Liechtenstein FMA is mandatory in the event of a serious operational or security incident. Moreover, if the incident affects or could affect the financial interests of its payment service users, the payment service provider must immediately inform its payment service users about the incident and about the measures they can take to limit the negative effects of the incident.

Contingent on the severity and extent of a data breach, it could reasonably constitute such an incident which would render it necessary to notify the Liechtenstein FMA.

9. ENFORCEMENT

The GDPR provides for administrative fines of up to (Article 83 of the GDPR):

- €10 million, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, for infringing provisions on the obligations of a controller, processor, certification body or monitoring body; and

- €20 million, or in the case of an undertaking, up to 4% of the total worldwide annual turnover for the preceding financial year, whichever is higher, for infringing provisions on the basic principles for processing, data subjects' rights, transfer of personal data to a recipient in a third country or international organisation, or non-compliance with an order or a limitation on processing by the supervisory authority.

The Liechtenstein Data Protection authority may impose a fine in case of a violation of the GDPR of up to CHF 11 million, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, for infringing provisions on the obligations of a controller, processor, certification body or monitoring body; and CHF 22 million, or in the case of an undertaking, up to 4% of the total worldwide annual turnover for the preceding financial year, whichever is higher, for infringing provisions on

the basic principles for processing, data subjects' rights, transfer of personal data to a recipient in a third country or international organisation, or non-compliance with an order or a limitation on processing by the supervisory authority. This difference of the threshold of the fines is due to the exchange rate of the Swiss Franc to the Euro.

Pursuant to Art 30 DDA violations in relation to AML may be punished with imprisonment of up to six months or a fine of up to 360 daily rates. However, such violations are in general not related to data protection aspects. Nevertheless, from a due diligence perspective, violations of data protection (e.g. commercial use of data received due to a required KYC/AML process) may pose an administrative infringement pursuant to Art 31 DDA which is punishable by fines of up to CHF 200,000.00 in addition to any fines based on the GDPR respectively the DPA.

As for banking institutions, Art 14 BA constitutes that the members of the executive bodies of banks and their employees and other persons working for such banks are obliged to maintain secrecy with regard to facts which have been entrusted to them or made accessible to them on the basis of business relations with customers. The obligation to maintain secrecy shall apply indefinitely. The Princely Court of Liechtenstein will punish any member of a governing body or an employee or any other person working for a bank or investment firm or as an auditor with imprisonment of up to three years, who violates the obligation of secrecy or who induces or attempts to induce others to do so.
if the violation does not constitute a criminal offence falling within the jurisdiction of the courts the Liechtenstein FMA may issue fines of up to 10 % of the highest total annual net turnover or gross income achieved in the last three financial years or up to twice the benefit derived from the infringement, insofar as this can be quantified and exceeds the total net turnover (gross income).
Withdrawing a license by the Liechtenstein FMA is only possible in case of serious offences.

10. ADDITIONAL AREAS OF INTEREST

Regarding the provision of core activities of a banking institution, personal data are inevitably also processed on a regular basis. Providing classical core banking activities can therefore not be seen in isolation from the simultaneous processing of personal data.

For this reason, the Article 29 Working Party has also determined that the processing of customer data in the regular banking business requires the appointment of a data protection officer.

With regard to data protection officers it should be noted that the top management level of a company may not at the same time function as a data protection officer.

This is ruled out in accordance with Art. 38 (3) and Art. 38 (6) GDPR, as the data protection officer would have conflicts of interest in this case. Art. 38 (3) GDPR stipulates that the data protection officer must report directly to the highest management level of the data controller or the processor. Art. 38 (6) GDPR stipulates in general that the data protection officer may perform other tasks and duties within the company, but not those that would lead to a conflict of interest.

Finally, it should be noted, that persons subject to due diligence have to ensure up-to-date and comprehensive training of their due diligence officers on matters concerning anti-money laundering as well as the countering of financing of terrorism and lastly data protection (Article 32 DDO). The profile of requirements for a data protection officer in a particular case will depend on the data processing operations carried out in a company and the need for protection of the personal data processed. In a company with complex data processing activities or a company processing large amounts of sensitive data, the data protection officer may need to have a higher level of expertise than in a company with less complex data processing activities (risk-based approach).