In their opinion, the **ESAs** praise how money laundering and the financing of terrorism can be prevented by using new technological solutions. However, they are only full of praise as far as the collection and review of large amounts of data are concerned. The demands they place on innovative KYC solutions is disproportionately higher than the requirements for traditional KYC methods. The opinion does not reflect an openness for innovation but a shocking hostility towards technology.

The Joint Committee of European Supervisory Authorities (these are the European Banking Regulator, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority – together the "ESAs") presented its views in its Opinion on the Use of Innovative Solutions by Credit and Financial Institutions in the Customer Due Diligence Process on 23 January 2018. This opinion serves as guidance for the national supervisory authorities as to how they should evaluate new technical solutions for

customer due diligence and monitoring and what requirements they should impose on such solutions as well as the obligated persons making use of these solutions.

It is expected that the national supervisory authorities will implement this guidance. It is therefore worth having a closer look at what this means for companies that are obligated persons in accordance with the German Anti-Money Laundering Act as well as for those offering innovative solutions.

ESAs and innovative KYC solutions. What is this actually about?

The identification of customers, i.e. the classic customer due diligence, is increasingly carried out online in today's age of digitalisation. This is due to the fact that if a customer first has to go to a bank or a post office to prove his identity, this is expensive for the provider and often causes the customer to lose interest. Providers of identification services via video live chat such as WebID or IDNOW fill this gap (hereinafter referred to as "video-ident providers"). However, there are further changes on the horizon. The eIDAS regulation also provides the possibility to set up centralised eID systems, whereby the customer only has to prove his identity once and his data can then be used by different companies (hereinafter referred to as "central data repository"). Alliances of different companies have already set up companies for this.

PayTechLaw has provided some commentary below on what the ESAs are recommending to video-ident providers or other innovative solutions in their recent opinion.

You want to build an innovative ID solution? The following must be noted:

Those continuing to ask their customers to come to the branch in person or to send them to the post office to use PostIdent, can continue doing so. However, companies wishing to use an innovative ID solution have to adhere to further rules according to the ESAs:

> Before introducing a new procedure, the company must carry out a rigorous risk assessment of the new solution. If this assessment is not able to dispel all doubts, the company has to continue operating the existing procedure (e.g. PostIdent or similar) in parallel. Up to now, doubts as to the quality of traditional processes have not led to a new solution having to be introduced and operated in parallel. The company must have a detailed understanding of the new procedure, both technically and legally, in order to be able to locate problems and to guide through the integration process. This understanding must also be present in senior management.

This is largely correct and to be supported. However, this raises the legitimate question as to whether senior management must also have an understanding of technical and legal details in respect of other matters.

The company must have a proper contingency plan in place if the new procedure fails. The ESAs therefore recommend always having at least two procedures implemented at all times. On the whole, it is always part of a reasonable risk management to have a contingency plan. However, the requirement to permanently provide a second identification solution is not required for traditional methods, even though they can also fail (due to strike, weather, computer failure, etc.).

The company must regularly review the provider as well as the innovative solution. If a serious error occurs, the company has to review the use of the innovative solution and stop using it, if necessary. This shows a lot of distrust. Any serious mistakes regarding the identification of a customer made by a bank branch or a post office, have so far not resulted in any calls to close down the branch or abandon the PostIdent process, but rather to rectify the error.

The ESAs believe that the innovative solution must be integrated into existing work processes and legacy systems. The aim is to ensure that all available information merges into a single system in order to provide a comprehensive overview of a customer. This requirement makes sense, however not only with respect to innovative systems, although it is only applied to them, which results in the fact that conventional systems do not necessarily have to merge into a single system.

The company has to examine whether, by way of or despite the integration of an innovative solution, it is able to develop a holistic view of the customer, which includes previous transactions, related accounts or customers, behavioural patterns and information from government registers, social media and other sources. There is no obligation to obtain further information about customers from other sources such as social media when using traditional methods. So why should this only apply if the identification process was carried out e.g. via video chat? It is clear that much stricter rules are applied here.

The ESAs believe that the cross-border provision of services increases the risk of money laundering/terrorist financing. For this reason, the payment service provider is required to record the customer’s location using fingerprints or GPS data from a mobile phone. In addition, the payment service provider is required find out why customers from other member states want to use its services. There is no such obligation to investigate the motives of customers with traditional KYC methods. Furthermore, I find it difficult to reconcile this requirement with the freedom to provide services which is guaranteed in the EU.

Retrofit? Retrofit!

The providers of innovative solutions must also take a close look at their products again because the ESAs have some surprises in store:

The employees of a video provider are to be trained to recognise faces to the extent that they realise when people look similar to the person in the picture on the ID document presented but they are not actually the owner of that ID card. Alternatively, technical solutions can be used to check if there is a match between the identity card presented and the holder. This training or the use of technical means to identify people does not

only make sense online, but particularly also at the counter of a bank branch or the post office. However, the instructions of the ESAs do not apply there.
Video-ident providers must introduce measures to ensure that no false or forged documents are not provided. Such measures can include, for example:

- built-in features which enable them to detect fraudulent documents based on their security features (i.e. watermarks, photographs, lamination, UV-sensitive ink lines) and the location of various elements on the document);
- an automatic comparison of the ID document presented with a sample ID card from the provider's database;
- limiting the type of acceptable identity documents to those that:
  - contain high-security features (e.g. fingerprints); or
  - contain a qualified electronic signature (particularly relevant for legal entities); or
  - provide a link to a government register (e.g. commercial register); or
  - are connected to a government-established central data repository or the notified electronic identification system as defined in the eIDAS regulation, if the scheme's assurance level has been classified as substantial.

None of these measures to detect false or forged documents has to be applied at a bank branch or post office counter. In my personal experience, the authenticity of ID documents is often checked there to a far lesser extent than with video identification. The reference to electronic signatures or electronic identification systems remains merely theoretical as it is not viable in practice. The population has neither the knowledge nor the hardware (nor the inclination) to use e-ID possibilities in accordance with the eIDAS regulation.

What providers of innovative solutions have to pay attention to…

Providers of innovative solutions also have to exclude that a customer is intimidated or threatened and only carries out the identity verification because of this. In the ESAs' view, this could be prevented through live chats with personnel trained in the basics of psychology, enabling them to spot abnormalities in the customer's behaviour. We can only hope that also bank and post office employees receive training in psychology.
Additionally, providers of innovative solutions must prevent that a person is on-boarded who is not who they claim to be (identity fraud). This has to be ensured through the following measures:

- the verification of the customer's identity on the basis of a notified electronic identification scheme, as defined in the eIDAS regulation, where the scheme's assurance level is classified as high; or

a combination of the following measures:

- the verification of a customer's identity based on a government-issued photographic document, combined with information obtained during the live chat with an employee and information obtained from the government or other reliable sources;
- automatic language recognition that can detect the native language of the customer;
- the requirement that all CDD documentation contains a qualified electronic signature created in line with the standards stipulated in the eIDAS regulation;
- the verification of a customer's identity on the basis of more traditional processes, such as sending a letter to the customer's verified home address.

What's left open

The opinion of the ESAs leaves open whether these measures have to be implemented at all times or only in cases where there is a suspicion of identity fraud. If they are intended as measures which have to be implemented at all times, then the ESAs might as well have written that they do not want any innovative solutions. Because if the consequence is that the customer can be identified by letter after all or only by means of an additional eID procedure which is not practical for the majority of the population, then this means that the preference is to return to the bank counter. And that the internet is only a fad.

Titelbild / Cover picture: Copyright © fotolia