Blog Post

N° 2/2018

eIDAS, PSD2, GDPR & Co

The European legal framework for digital identities and communication

Andrea Müller

Dr. Andreas Windisch

ASQUARED

asquared Blog Post N° 2/2018

February 2018

In recent years, the EU has launched a series of regulations and directives that will work together and interact to set the framework for the Digital European Economic Area with a focus on identity and personal data. Individual frameworks will not come into force until 2019, the next two years mark the gradual transition into the target image.

Introduction

The handling of identity data and personal data is subject to state regulation. In recent years, several legislative initiatives have been launched in Europe, each with a different focus, setting the framework for digital identity services. The discussion processes and legislative procedures for the initiatives dragged on for several years, and the Europe-wide implementation of the agreed guidelines will also take a longer period of time. The ePrivacy regulation is still in the legislative process. The graphic below gives a rough overview of the regulations' entry into force.

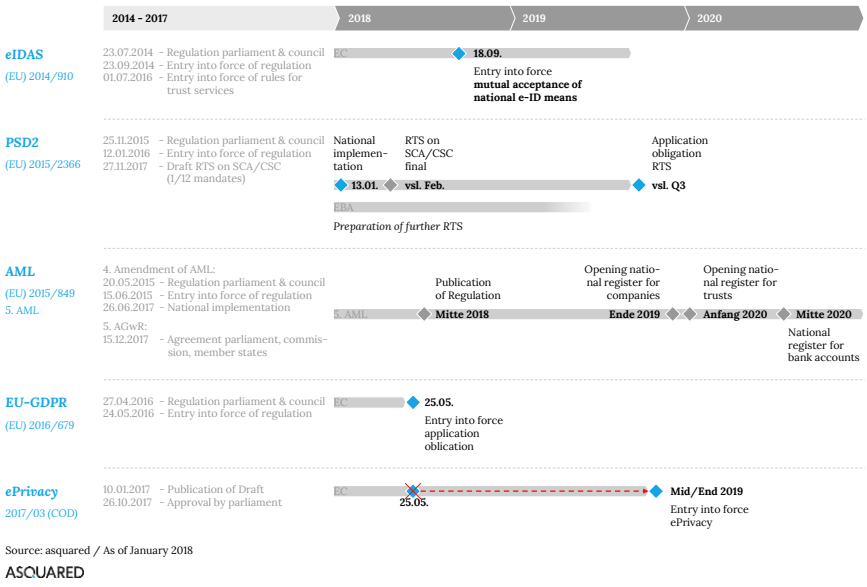

Figure 1: *Overview of regulatory requirements in the field of e-identity and communication*

These regulations, individually and in interaction over the next two years, will significantly change the framework for digital identity services in Europe. The eIDAS sets the framework for the interoperability of identity and trust services with a view to their use in national administrative procedures, but also provides a reliable framework for application in the economic sector. PSD2 opens the online banking for third-party providers, including the retrieval of data about the account holder. The aim of the GDPR and the ePrivacy regulation is to regulate the handling of personal data throughout Europe in a uniform manner.

eIDAS – A single European framework for electronic business processes between public authorities and citizens and companies

The eIDAS Regulation (**e**lectronic **Id**entification, **A**uthentication and Trust **S**ervices) aims to create a robust European legal environment for secure and trustworthy electronic business processes in the public sector. The electronic interaction between citizens, companies and authorities is to be improved and made possible transnationally by means of the Regulation, which came into force in September 2014. The eIDAS distinguishes between two areas: electronic identification and electronic trust services. For both areas, a series of implementing acts were adopted by September 2015, which regulate details of the implementation of the identity and trust services. In addition to the minimum standards for services, this also includes regulations for the exchange of information between the countries and the establishment of the system for the interconnection of electronic identification systems (eIDAS nodes). Providers of eIDAS-compliant services must undergo testing by dedicated conformity assessment bodies to be permitted to provide trust services and to be included in the list of national trust service providers. The list is kept by a national authority, in Germany the Federal Network Agency is responsible for this task. The Trusted List of Trusted Lists (LOTL) provides a Europe-wide overview of all audited and approved national providers.

The rules of the eIDAS for trust services have been in force since 01.06.2016. According to eIDAS (Chapter III Art. 13 - Art. 45), this includes electronic signatures, seals, time stamps, validation, enrolment, delivery and safekeeping services as well as website authentication services. Article 25 of the eIDAS equates qualified electronic signatures (QES) to a handwritten signature, regarding their legal effect. If this is based on a certificate issued in a member state, the signature must be recognized in all member states. It is essential that the eIDAS no longer necessarily requires the presence of a signature card in the user's hand. Signatures can also be created if the signature file resides on secure servers of the trusted service provider. This significantly reduces the effort required to use a QES and makes its widespread use possible. However, this does not mean that all hurdles have been overcome; issuing the certificate for a QES still requires the user's identity check in presence or an electronic identification device at security level "substantial" or "high".

EU member states can notify electronic means of identification on a voluntary basis. If these means of identification have passed the notification procedure successfully, they shall be recognized - starting from 29 September 2018 - no later than 12 months after the publication of the notification in the administrative procedure of the Member States in accordance with the notified confidence level. Germany was the first country to undergo the notification procedure. The notification of the online identification function

of the German ID card and the residence permit at the highest possible level of confidence was published on 26.09.2017 in the Official Journal of the EU Commission. Italy was the second country to apply for pre-notification of the Italian eID scheme *SPID (Sistema Pubblico per la gestione dell' Identita Digital*) on 24.11.2017 and is in the notification process, which will not be completed before May 2018.

For eIDAS to be able to develop the intended effects on communication between citizens and businesses and public administrations, a broad participation of all member states is required. Each Member State bears responsibility for its citizens for the promotion and/or development of eIDAS-compliant identity and trust services and for the digitization of its own administrative procedures. Their readiness to promote digitization of administrations both nationally and internationally has been confirmed by the Prime Ministers of the EU Member States and the EFTA countries at the ministerial meeting in Tallinn. Together, they signed the "Declaration on eGovernment" on 6 October 2017. Aligned to five basic principles, the declaration includes an action plan to establish open, efficient, cross-border, interoperable, easy-to-use, digital public services by 2022. Whether the declaration is more than just a political signal, remains to be seen within the coming months and years. The declaration explicitly emphasizes the importance of eGovernment for the digital single market and digital innovation, and hence economic development in European countries.

Amendment to the anti-money laundering directive - digitization of KYC processes

A particularly close interplay exists between public digital e-identity infrastructure and services of the financial sector: The identification of the customer is a mandatory part of the onboarding processes for customers of financial institutions. In this respect, it is not surprising that the proposal for a Directive on the new anti-money laundering directive agreed by representatives of the European Parliament, the European Commission and the Council of the Member States in December last year, makes explicit reference to the use of electronic means of identification in accordance with eIDAS for KYC processes. In addition, a European group of experts has been set up to deal with the cross-border use of electronic identifiers for KYC processes.

PSD2 - New business models for banks and third-party service providers

With the use of qualified website certificates and qualified seals for the identification of third-party service providers (TPPs), the second amendment to the Payment Service Directive (PSD2), effective since January 2018, also applies to the structures created by the

eIDAS. The PSD2, which obliges banks to grant regulated third-party service providers access to the payment accounts they manage in online banking, has been the subject of many discussions for years. And even if the PSD2 came into force in January, it is still not fully effective. The EBA has 12 mandates to develop PSD2 tools related to technical standards, reporting guidelines, the register to be established, consumer protection and other topics. With the entry into force of PSD2, three of the instruments will be applicable, others will be in preparation or will enter into force after a transitional phase for which the EBA made recommendations in December 2017. The transition phase also applies to the intensively debated Regulatory Technical Standards (RTS) for strong customer authentication (SCA) and secure communication (CSC). The Consultation Paper for RTS on SCA and CSC, published in August 2016, provided EBA with 224 responses - the highest number of responses ever obtained in such a process. Following an intensive consultation process, the final draft of the RTS was handed over by the EBA to the EU Commission on 27.11.2017. The RTS are therefore expected to take effect towards the end of the third quarter of 2019 and banks will gain time to adjust.

In the discussion on the PSD2, two topics are in focus: The paradigm shift in banking in general - this refers to the formation of value-added networks in the area of financial services promoted by the pressure towards API banking - and the changes in payment traffic in particular. The Payment Initiation Service (PIS) enables the initiation of payments from online payment accounts. However, the changes resulting from access to the account information service (AIS) are at least as relevant for electronically transmitted verified identity data and banking transaction data. By accessing the account interfaces, TPPs may, with the consent of the customer, retrieve both transaction data and account holder data, whereby the data retrieval permitted under the PSD2 being restricted to the data achievable in the online banking. These data must be transmitted to TPPs without charge to banks with the consent of the account holder. Based on established freemium models, banks can offer fee-based services that enrich this data with additional bank-specific data and, at the customer's request, transmit it via API to TPPs. With *e-identification*, *Giropay-ID* and *identity™ Giro* functionally comparable offers already exist. The possibility of providing enriched or processed data also relates to transaction data. Here, the opposite is also conceivable, customers may not want to transmit a third party all information derived from the transaction data information. The custom-fit provision of data on customer request forms a direct possibility for monetization for banks and, moreover, the possibility of offering services that integrate the banking data, either alone or together with cooperation partners.

Although an API is not yet a business model, the discussion about the PSD2 API provides insight into possible business models of different stakeholders. The PSD2 itself does not provide an API standard as well as the RTS does not define a technical API standard. In response to the PSD2, several initiatives have evolved in the market that are developing

a PSD2 API standard. These include the British *Open Banking Initiative*, the *French Stet Group* and the *Berlin Group*, to only name a few. The PSD2 API has been the topic of many discussions over the last few months, with the discussion focusing not on the pros and cons of the proposed standards, but on whether in parallel to access via API screen scraping should continue to be allowed for third-party providers. The requirement to maintain the use of this access method is justified by the companies grouped together under "Future of European Fintech" on the grounds that their access will be impeded due to insufficient availability of the Bank's APIs. For this reason, the FinTechs demanded the continued existence of Screen Scraping at least as a fallback solution. The RTS have developed a compromise in that they provide, that banks can be relieved of the obligation to provide a fallback solution if their API adheres to certain performance metrics. In this case, the access may only be offered via the API and banks and customers remain in the driver seat and can transparently control the access to the banking data.

The EU-GDPR - Strict rules for the processing of personal data in Europe

The General Data Protection Regulation (DSGVO) is an essential building block for the establishment of the digital single market. It aims at the protection of personal data, as well as the guarantee of liberal data traffic between the member states. Already in January 2012, the European Commission presented the first proposals for a reform of the data protection law. The proposals were discussed intensively both within the regular legislative procedure, as well as in business, science and civil society. After completion of the consultations of the ordinary legislative procedure, the GDPR was approved by the European Parliament on 14.04.2016 and entered into force on 24 May 2016. Following a two-year transitional period, the regulation will become directly effective on 25 May for businesses and administrations in all EU Member States.

The general principle for the processing of personal data remains a prohibition with conditional approval - the processing of personal data is therefore always only permissible, if a consent or an exception mentioned in the GDPR exists. The GDPR is based on the structure and basic principles of the predecessor ordinance but extends these to a few key points. Among others, these enhancements include the following:

Market place principle (Art. 3)

The GDPR applies to all companies operating in the European market. It is not the location of the company or the place of data processing that matters, but the fact that the offer is aimed at one or more national markets in the EU. It also applies to non-European companies and ensures a level playing field for companies offering services on the European market.

Privacy by Design / Privacy by Default (Art. 25)

The Privacy by Design / Privacy by Default principles are expanding the existing principles of data avoidance and data economy, and explicitly introduce "data protection through technology and data protection-friendly presettings". They make demands on the design as well as the implementation of products and services. Application presets may only be targeted to the data necessary for the purpose. The principles must be considered in the collection, processing and storage of data.

Strengthening of sanctions and fines (Article 83)

Violations of the GDPR can be punished with penalties of up to € 20 million or up to 4% of the total worldwide annual turnover in the previous financial year; whichever value is higher. The significant increase in financial risks is aimed at increasing the weight of data protection and thus improving living standards.

Deadlines for data protection incidents (Art. 33)

Data protection incidents must be reported to the responsible supervisory authority without delay, if possible within 72 hours. If the incident concerns a party engaged for processing the data, he must inform the client immediately. Records must be kept of data protection incidents that enable the supervisory authority to check compliance with the provision.

Conditions for consent to the processing of personal data and conditions for the consent of a child (Art. 7 and 8)

If companies process personal data, they must have explicit consent from their customers and must be able to provide evidence of this. A consent by a child is only considered lawful if the child has reached the age of sixteen. Member States may provide for a lower age limit, but this may not be less than the age of thirteen.

Right to cancellation and data portability (Art. 17 and 20)

In the future, companies will have to delete personal data at the request of those affected. Customers also have the right to take their data from one service provider to another.

With the expanded information and recording obligations, as well as the tightened sanction possibilities on the company side and strengthening of the user rights on the other side, the GDPR aims at an increased attention for data protection relevant topics and standards in the handling of personal data. The differences in privacy policy evaluation existing through regulations and/or legal practice within Europe will be removed. They

are being replaced by DSGVO, a uniform regulation throughout Europe, which sets a uniform framework for all companies active on the European market.

ePrivacy Regulation - Data Protection for Digital Communications

The aim of the ePrivacy Regulation is to complement the GDPR in the field of electronic communications. So far, the provisions of the 2002 ePrivacy Directive and the 2009 Cookie Policy have complemented the Data Protection Directive. With the transfer of these regulations into GDPR, which directly and uniformly is effective in Europe, the area of electronic communication will also be redefined in a uniform manner in order to set the framework for the digital European single market. In addition, electronic communication has changed dramatically since the entry into force of the guidelines. This change should also be taken into account with ePrivacy.

For e-identity solutions, the ePrivacy Regulation is highly relevant as it explicitly focuses on the protection of electronic communications data, not just the data exchanged over the telephone, but also over the Internet. Even for these data the prohibition with conditional approval from the DSGVO is to be applied in the future. The collection and processing of the data must be covered by an exception or explicitly permitted by the user. This does not only apply to cookies, but generally to all solutions for the identification of the user. IT solutions must be delivered with data protection-friendly basic settings, communication services should enable secure end-to-end encryption.

There were intensive debates about the regulations of the ePrivacy Directive in the last year. While proponents point out strict rules on the privacy implications of data collection and processing, possible discrimination (keyword scoring), and impact on societal opinion-forming processes, critics see at risk both European economic development as a whole and individual sectors of the economy in particular.

On 26 October, the EU Parliament adopted the draft of the ePrivacy Regulation. However, this approved draft may be changed further in the trialogue negotiations between the European Commission, the European Parliament and the Council of the European Union. As the protection areas of the GDPR and the ePrivacy overlap, initially both regulations should take effect at the same time. However, this goal will no longer be achieved: Currently, ePrivacy is assumed to take effect in 2019.

Conclusion

In Europe, eIDAS, PSD2, DSGVO and the ePrivacy Regulation have been a major driver in recent years for setting common European frameworks for the exchange of personal

data and identity data. In doing so, Europe is sending a clear signal towards uniform and reliable legal regulations for all European countries. The regulations will gradually take full effect due to the staggered onset of their effectiveness. However, in doing so, the foundation for the development of offers is largely laid.

Sources

1 Official Journal of the European Union, Regulation (EU) No 910/2014 of the European parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, downloaded on 21.01.2018, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910

2 European Union, Connecting Europe Facility Trusted List Browser, downloaded on 21.01.2018, https://webgate.ec.europa.eu/tl-browser/#/

3 Official Journal of the European Union, Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, downloaded on 21.01.2018, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1517496863085&uri=CELEX:52017XC0926(02)

4 Ministerial Declaration on eGovernment - the Tallinn Declaration, downloaded on 21.01.2018, https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovernment-tallinn-declaration

5 European Commission, Proposal for a directive of the European parliament and of the council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, downloaded on 21.01.2018, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0450&from=DE

6 European Commission, Commission Decision of 14.12.2017 setting up the Commission expert group on electronic identification and remote KnowYour-Customer processes, downloaded on 21.01.2018, http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=36277&no=1

7 EBA, EBA publishes Opinion on the transition from PSD1 to PSD2, downloaded on 21.01.2018, https://www.eba.europa.eu/-/eba-publishes-opinion-on-the-transition-from-psd1-to-psd2

8 The Future of European FinTech, Manifesto for the impact of PSD2 on the future of European Fintech, downloaded on 21.01.2018, https://www.futureofeuropeanfintech.com/assets/Manifesto-for-the-impact-of-PSD2-on-the-future-of-European-Fintech.pdf

9 European Commission, Directive 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication,

downloaded on 21.01.2018, http://ec.europa.eu/finance/docs/level-2-measures/psd2-rts-2017-7782_en.pdf

10 Official Journal of the European Union vom 04.05.2016, VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), downloaded on 21.01.2018, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&rid=1

11 Das Europäische Parlament, Legislative Observatory, Procedure File zu 2017/0003(COD) "Respect for private life and the protection of personal data in electronic communications", downloaded on 21.01.2018, http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=&reference=2017/0003(COD)#tab-0

Authors

Andrea Müller disposes of many years of experience in the design of digitization and transformation processes in both the banking and financial sector as well as the manufacturing industry. As an IT business engineer and economist in foreign trade she has acted in responsible positions in industrial and consulting firms.

Dr. Andreas Windisch is Managing Director at asquared. As a certified computer scientist and with a doctorate in engineering, he acted in leading positions in automotive, technology and consulting firms and disposes of many years of experience in the field of IT transformation management - especially in the banking and financial services sector.

About asquared

Asquared is a Berlin-based consulting firm. Our work focuses on developing practical solutions for the regulatory, technologically and/or socially induced change, associated with direct application and confirmation in an industrial environment.

Our attention is focused on business and technology and their interaction. Reaching from the reorientation of strategies, over the (re)design of products and services to the operationalization - our work focuses on shaping change. On all levels.

We present selected insights of our theoretic and practical research work to a broader audience in the form of publications and lectures.

asquared GmbH
Pappelallee 78/79
10437 Berlin - Germany

Telefon +49 (0) 30 22 66 79 60
E-Mail contact@asquared.team

asquared.company
asquared.blog
twitter.com/asquaredgmbh
instagram.com/asquaredgmbh
linkedin.com/company/asquared