Strong Customer Authentication in Online Payments Under GDPR and PSD2: A Case of Cumulative Application

Danaja Fabcic(✉)

Centre for IT & IP Law, KU Leuven, Leuven, Belgium
danaja.fabcic@kuleuven.be
https://www.law.kuleuven.be/citip/

Abstract. Authentication is the process of confirming the user's identity before the payment can be performed. It contributes to cybersecurity by preventing access by unauthorised parties. However, in e-payments the authentication differs from traditional identity checks since it is performed online and remotely. This paper explores the relationship between two important legal instruments on authentication in payment services: General data protection regulation (Regulation 679/2016) and the Second payment services directive (Directive 2015/2366). This paper shows that while the relationship between the two instruments can be considered unclear, previous research and European soft law favour cumulative application, and not a lex specialis and lex generalis relationship. These findings are then discussed in the context of implementing authentication procedures in compliance with the rules of the GDPR, with a focus on the identity of the controller, legal basis for implementing authentication, and the security requirements under art. 32 of the GDPR. Based on the "means reasonably likely" test from the Breyer judgment, we assume that PSPs could be considered controllers even when processing pseudonymised credentials. Legal grounds to process personal data in an authentication procedure are either performance of a contract or legitimate interests of the controller, insofar as the necessity criterion is met. Relying on legal obligation is, however, more doubtful. Finally, exceptions to strong customer authentication bring their own cybersecurity considerations, since complexity of security systems can lead to more vulnerabilities. When PSD2 and GDPR are both applied, it may mean that compliance with the higher standard is required, which is enabled by the optional nature of art. 18(1) of the RTS.

Keywords: Strong customer authentication · Data protection · Payment services · Cybersecurity

Funding disclaimer. The research for this paper was carried out in the context of two Horizon 2020 projects: FENTEC (Grant agreement no. 780108) and KRAKEN (Grant agreement no. 871473).

Published by Springer Nature Switzerland AG 2021
M. Friedewald et al. (Eds.): Privacy and Identity 2020, IFIP AICT 619, pp. 78–95, 2021.
https://doi.org/10.1007/978-3-030-72465-8_5

1 Introduction

Online shopping is a growing industry in Europe – Eurostat reports that between 2009 and 2019, the number of online shoppers has doubled, and 60% of Europeans buy online at least once a year. During the first 2020 lockdown, there was an estimated 17.4% growth in online and mail orders[1,2]. Online shopping is facilitated by electronic payments, the online transfer of money through a variety of payment services providers (PSPs). However, identification of online shoppers cannot be performed in person, meaning that PSPs need to counter the risk of fraud, impersonation or unauthorized access to the device [3,11]. As the perpetrators have begun to use more complex and more successful equipment to carry out social engineering attacks, PSPs respond by adopting stronger security measures [13]. These often include authentication, a process intended to confirm the user's identity by the PSP before the payment can be performed [5].

In the European Union, authentication in online payments falls under the Second payment services directive (Directive (EU) 2015/2366, hereafter: PSD2)[3], which requires PSPs to implement strong customer authentication (SCA); or as a security measure under the General data protection regulation (Regulation (EU) 2016/679, hereafter: GDPR)[4] if personal data are processed.

The goal of this paper is to provide clarity on the interplay between GDPR and PSD2 and illustrate their cumulative application on the example of SCA in online payment services within the European Union. The knowledge can be used to help understand lawyers, engineers and computer scientists what are the legal requirements for SCA under these two frameworks. This will contribute to understanding how to best achieve compliance with authentication requirements for actors in e-payments industry, especially those who provide payment services.

The work will follow the existing doctrinal work on the interplay of PSD2 and the GDPR, taking into account applicable legislation and interpretative guidelines by expert bodies, in order to answer the following research question: "What is the relationship between the General data protection regulation and the Second payment services directive; and what is its impact on compliance of strong customer authentication processes?" Methodologically, the paper is based on doctrinal and black letter research.

[1] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Impact_of_Covid-19_crisis_on_retail_trade, last accessed 2020/09/12.

[2] https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20200420-2, last accessed 2020/09/12.

[3] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. OJ L 337.

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

This paper is structured as follows. The first part is descriptive: the legal framework of authentication in EU payment services law is presented, drawing upon the analysis of legal provisions, doctrinal work and soft law documents. In the second part, the relationship between the GDPR and the PSD2 is analysed *in abstracto*, and *in concreto* on the example of authentication.

2 Strong Customer Authentication in EU Legal Framework

European Union regulation of cybersecurity started out in soft-law document: recommendations, communications and guidelines issued by institutions, especially at the political levels (e.g. European Council). Jasmontaite et al. [14] provide an overview of soft law documents issued in the period 2000–2016. The authors note that there is no holistic approach to cybersecurity at the EU level; instead, various frameworks are used, such as network and information security measures, data protection and privacy in electronic communications, and cybercrime legislation.

A possible reason is that the Union has limited competences in the area of cybersecurity under the conferral principle as set out in art. 5 of the Treaty on European Union. (TEU)[5] Under this principle, the EU can only act under the competences conferred upon it by the member states, and the member states retain the other competences. Hence, the EU is restricted to regulating cybersecurity in the context of internal market. Since it is a comparatively new legislative area, some flexibility is necessary. That is achieved by combining minimum harmonisation directives with full harmonisation regulations [12].

EU cybersecurity regulation is based on trade-offs, such as security and utility (the more secure something is, the less usable it is), or privacy against another valuable goal in the e-health, business or finance domain [28]. Authentication is a good example of usability versus security, since users typically don't like complicated passwords, and yet maintaining cybersecurity is an important objective for stakeholders involved[6].

Regulation of cybersecurity in payment services is likewise a relatively new area of EU legislative effort. The two main instruments, which impose cybersecurity obligations and safeguard data in payment services, namely the Second payment services directive (PSD2) and the General data protection regulation (GDPR), were adopted within the context of internal market regulation.

The regulation of electronic payments is layered, following the value chain of payments, (mobile) device, retail and technology, meaning that each subset is subject to a specific set of rules [16]. In this section, the legal framework on authentication in online payment services in the EU is presented.

[5] Treaty on European Union. Official consolidated version. OJ C 326/12.

[6] https://social.techcrunch.com/2018/12/25/cybersecurity-101-guide-two-factor/, last accessed 2020/09/12.

2.1 General Data Protection Regulation (GDPR)

The GDPR applies to processing of personal data, which are any information relating to an identified or identifiable natural person (data subject). It was adopted by the European Parliament and the Council in 2016, and has been in force since May 25, 2018. Data protection is an important objective of the European Union: the GDPR was adopted with the aim of contributing to protection of fundamental rights, the area of security, freedom and justice, as well as facilitating exchange of data in the burgeoning economic union of the internal market (recital 2 of the GDPR). The Regulation lays down a comprehensive, cross-sectoral regime for protection of personal data.

Processing is only allowed if there are valid legal grounds, exhaustively listed in art. 6. These are the consent of the data subject, or if processing is necessary for the performance of a contract, compliance with a legal obligation, to protect the vital interests of the data subject or of another natural person, for the performance of a task carried out in the public interest or in the exercise of official authority, or necessary for the purposes of the legitimate interests pursued by the controller or by a third party, unless these interests are overridden by the fundamental rights of the data subject. According to WP29, only one legal basis applies to a data processing activity, and no other legal grounds may be considered.

The central burden of compliance with the obligations contained in the GDPR lies with the data controller, the entity which, alone or jointly with others, determines the purposes and means of the processing of personal data (art. 4(7)). The controller is responsible for implementing appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in a compliant manner (art. 24). This includes the obligation to implement data protection by design and by default (art. 25(1) and (2)), to choose its subcontractors (data processors) with due diligence (art. 28), and to lay down appropriate security measures (art. 32).

In the payment services, the GDPR might apply to issuing and verifying credentials during the authentication process. Credentials can fall under the definition of data processing since they are on principle tied to one specific user. If the user is an identified or identifiable individual natural person, then they are a data subject with-in the meaning of art. 4(1) of the GDPR. This is especially the case if biometrics are used as the second authentication factor.

The GDPR defines biometric data in art. 4(14) as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person; these data are then used for unique identification of that natural person. If these data are used for uniquely identifying a natural person, then they fall into a special category of personal data under art. 9 of the GDPR (also called sensitive personal data). Their processing is subject to a stricter regime, and is in principle not allowed unless strict conditions are met, such as explicit consent or other criteria laid down in national legislation. Mobile wallet and mobile bank providers, such as Apple Pay

and Google Wallet, give their user a choice between biometric authentication or using a PIN code [11].

2.2 Second Payment Services Directive (PSD2)

PSD2 is a full harmonization directive adopted by the EU in 2015 with the objective of closing the regulatory gaps while at the same time providing more legal clarity and ensuring consistent application of the legislative framework across the Union. The instrument aims to benefit operators of payment services by opening up the market, as well as enhancing consumer protection by providing for safe and secure payment services. Among other goals, the PSD2 addresses the security challenges of ever more complex online payments. In its Recital 7, it states that safe and secure payment services constitute a vital condition for a well-functioning payment services market. Users of payment services should therefore be adequately protected against such risks.

PSD2 applies to payment services provided by payment service providers within the Union. The exhaustive list of payment services is laid down in Annex I to the directive, and includes eight different types of payment services, such as placing cash on a payment account, or execution of payment transactions, including transfers of funds on a payment account, as well as payment initiation services and account information services. A payment service provider is an entity, which falls into one of the six categories laid down in art. 1(a) of the directive, for example: credit institutions as defined in art. 4(1) of Regulation (EU) No 575/2013[7], electronic money institutions within the meaning of art. 2 of Directive 2009/110/EC[8], or payment institutions authorized under Chapter 1 of Title II of the PSD2. The PSD2 also introduces two new types of PSP: an account information service provider, and a payment initiation service provider.

An account information service provider is an online service which provides consolidated information about different payment accounts held by one user (art. 4(16) of PSD2). For example, these are apps that help with budgeting, spending monitoring and financial planning [9][9].

A payment initiation service provider is a service which initiates a payment order at the user's request (art. 4(15) of PSD2), thus providing an alternative to users not possessing or not wishing to use credit cards. For example, a payment initiative service provider is Sofort in Germany[10], and Bancontact in Belgium[11].

[7] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012. OJ L 176.

[8] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC. OJ L 267.

[9] https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_15_5793, last accessed 2020/09/14.

[10] https://www.sofort.de/, last accessed 2020/09/14.

[11] https://www.bancontact.com/en, last accessed 2020/09/14.

The PSD2 has a dedicated chapter on cybersecurity. Its Sect. 5 is entitled 'Operational and security risks and authentication'. Under art. 95, PSPs must implement mitigation measures and control mechanisms to manage the operational and security risks (art. 95(1) of PSD2), and to report those mechanisms regularly to the competent authority (art. 95(2) of PSD2).

Under the first paragraph of the article, PSPs are required to establish a frame-work with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services they provide. The establishment and maintenance of effective incident management procedures, including for the detection and classification of major operational and security incidents, is part of the mitigation and control framework. The second paragraph obliges PSPs to report those mechanisms to competent authorities regularly. More specifically, PSPs need to provide an updated and comprehensive assessment of the operational and security risks relating to the payment services they provide, and report on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

The third paragraph gives EBA the mandate to issue guidelines on the establishment, implementation and monitoring of the security measures; the guidance was given in late 2019 [4].

Art. 97 lays down authentication obligations. PSD2 defines authentication in art. 4(2) as a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials. Personalised security credentials mean personalised features provided by the payment service provider to a payment service user for the purposes of authentication (art. 4(31) of PSD2).

Strong customer authentication (SCA) is defined in art. 4(30) as an authentication based on the use of two or more elements. Those elements can be knowledge (something only the user knows), possession (something only the user possesses) or inherence (something the user is); the elements must be independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data. However, PSD2 explicitly requires PSPs to put into place only user or customer authentication, whereas authentication of other actors may fall under general requirements of art. 95. It is unclear why the legislator has taken this decision given the contribution of authentication to cybersecurity of PSPs.

PSPs are required to apply strong customer authentication in three instances, when the payer (a) accesses its payment account online; (b) initiates an electronic payment transaction; or (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

2.3 Regulatory Technical Standards (RTS)

Regulatory Technical Standards (RTS) for strong customer authentication and common and secure open standards of communication were adopted by the Commission on the basis of European Banking Authority's activities (Commission

delegated regulation 2018/389)[12]. While the term "standard" implies voluntary compliance, their adoption by the Commission means that the RTS are a legally binding instrument and PSPs need to comply with them as of September 2019.

One of the goals of the RTS is to specify the requirements of SCA. More specifically, SCA should be applied each time a payer accesses its payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuse. To counter the risk, an authentication code which should be resistant against the forgery or disclosure, should be issued (recital 1 of RTS).

Like PSD2, the RTS describe strong customer authentication as procedure (art. 1(a) of RTS). In order to provide strong customer authentication, payment provider must ensure that authentication is based on two or more elements factors. As in the PSD2, these elements are categorised as knowledge, possession and inherence, and the characteristics of those elements described in detail in art. 6, 7 and 8 of RTS. The elements of authentication need to be independent from each other, meaning that if one of them is breached, the others are not disclosed as a result (art. 9 of the RTS).

There are some exceptions to requiring two-step factor authentication, for example for low-value transactions. These are one-off transactions below 30EUR, or transactions whose cumulative value is below 100EUR, and there can be at most five transactions until SCA is required again (art. 16, paras a-c of RTS).

3 Theoretical Overview of the Overlap Between PSD2 and GDPR

PSD2 has been understood in the context of open banking, the opening up of traditionally bank-dominated industry to new players and actors (often broadly referred to as fintech). Open banking on the one hand improves the customer experience; on the other, it forces the 'traditional' financial industry to invest significant resources in technological innovation and in the creation of new technical and compliance processes [19]. The adoption of the revised directive in 2015 was predicted to enhance harmonization, encourage growth and innovation, as well as ensure security and consumer protection, and enable the fight against payment fraud [27].

The framework contained in the PSD2 interacts with the GDPR when personal data are processed. The relationship between the two frameworks has been analysed from the perspective of security of third party access to accounts under art. 66 and 67 of the PSD2 [27], their interaction in an open banking context and the opportunities they bring to new fintechs [20], the re-use of personal data by PSPs under the purpose limitation principle [25], and finally the relationship

[12] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 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. C/2017/7782 OJ L 69.

was thoroughly analysed by the EDPB, with a strong focus on data protection issues [9].

In July 2020, the EDPB issued its Guidelines 06/2020 on the interplay of the PSD2 and the GDPR (hereafter: the Guidelines 06/2020) [9], which answered some of the above questions. The document was open for consultation to the public until September 2020; the final version of the guidelines has not been made available yet.

The board stresses that framework contained in the PSD2 establishes a link be-tween data protection, consumer protection and competition law, the focus is given above all to the data protection aspects. The document further analyses the position of PSPs within the context of the GDPR, explaining that depending on the context the PSPSs can act either as controllers or processors. In order to process personal data lawfully, they can invoke the legal grounds of necessity to perform a contract, legal obligation to grant access to the account under art. 66 of the PSD2, or further processing of already lawfully collected data. The Guidelines 06/2020 also tackle the notion of explicit consent, which differs under art. 94(2) of the PSD2 and arts. 6, 7 and 9 of the GDPR. The explicit consent contained in art. 94(2) of the PSD2 cannot be valid legal grounds for data processing; instead, it can play a role as an additional data protection safeguard for the data subject. More specifically, in para. 36 the board explains that the explicit consent under the PSD2 has a contractual nature, meaning that the PSPs must disclose exactly what kind of personal data will be processed, and for which specific purposes. Thus, the requirement of explicit consent under art. 94 of the PSD2 guarantees transparency and gives more control to the user of the payment service (para 38).

The Guidelines 06/2020 emphasize that the lack of appropriate security measures in a PSP may have dire consequences: financial losses for the company, loss of customer trust, and if the PSP is a bank, then the customers cannot use their cards to access their funds. For example, a recent incident in a South African bank following the theft of a master key led to the bank recalling 12 million bank cards[13]. Moreover, extensive financial records can offer a very detailed insight into an individual's life. For example, donations to political parties, annual membership fee in a labour union, frequent visits to a swingers club, or settling of medical bills for a specific health condition. Using big data techniques, payment records can also show minute behavioural pattern, all of which may lead to a higher risk of fraud [9]. Hence, the board recommends that PSP implement the principle of data minimisation as part of their data protection by design approach and to contribute to the security of personal data under art. 32 of the GDPR.

The access to data under art. 66 and 67 of the PSD2 was predicted to reduce online payment costs, and give rise to new business models, while art. 97 aims to improve client authentication and security [18,20]. Data portability and screen

[13] https://www.zdnet.com/article/south-african-bank-to-replace-12m-cards-after-employees-stole-master-key/, last accessed 2020/09/12.

scraping are key measures to facilitate open banking. However, opening up the data held by banks to new players also brings cybersecurity considerations [20].

PSPs rely on computer infrastructure in order to carry out online payments. This means that a cyber-incident could jeopardise the functioning of ICT systems, pose risks to data integrity and cause other impacts stemming from cyber-incidents that go beyond financial losses on stock markets [1,4].

The cybersecurity of the payment depends on the security measures adopted by different actors throughout the payment chain ecosystem. Carrying out security risk assessments and including security measures into the general governance can con-tribute to overall security. Specifically, designing application with security in mind, as well as using high quality end-to-end encryption (SSL/TLS), are minimum security measures that can be adopted at different points in the payment chain, by the users, customers and the merchants [5,11]. Despite the recommendation for the users to adopt security measures, the ultimate responsibility for a well-designed system should not lie on the individual user [22].

Traditional financial institutions should also implement strong controls over privileged system access, meaning accounts with elevated system access entitlements, such as administrator accounts. Measures should follow the need-to-know principle based on strong authentication [4]. ENISA recommends adopting measures on the side of users as well as merchants, and the PSPs themselves should ensure secure development of the payment service [11], in accordance with the emerging principle of security by design [7].

There are two types of authentication required during a payment process: first, authentication of the device and secondly, that of the user [11]. Art. 4(29) of the PSD2 states that authentication is a procedure which "allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials" . It is not clear whether this definition includes the authentication of the device.

Poor authentication is a risk, since it can lead to unauthorized payments, as well as disclosing the underlying sensitive payment data, such as credit card information and personal credentials to unauthorized third parties. Since security of online payments relies to a large extent on the secrecy of tokens and cryptograms, strong authentication can be an effective protection measure [11]. However, while authentication is a useful counter-measure, in itself it is not sufficient and must be paired with other security measures to counter ICT and security risks [4].

Implementing strong authentication is also a motivated business decision. As the banks lose their traditional monopoly over the payment market, they also lose the control and their exclusive access to customer data. In order to prevent fraud and unauthorized access to payment data, strong authentication measures are necessary. However, under the PSD2 banks are placed in an awkward position, since they are required to ensure data protection of their customers' data, and prevent fraud, while needing to trust that the PSPs have adequate authentication mechanisms without banks being able to verify them [18,27].

4 Relationship Between GDPR and PSD2

4.1 Relationship Between the PSD2 and GDPR – Article 94 of PSD2

Data protection in payment services is discussed in Recital 89, and art. 94 of the PSD2. While other articles, especially those on access to information by payment services providers in art. 66 and 67, contain a link to data protection law [27], this is the only explicit rule on the subject.

According to art. 94, processing of personal data by payment systems and payment service providers is *permitted when necessary* to safeguard *the prevention, investigation and detection of payment fraud.* Individuals must be informed on the processing of personal data for those purposes with accordance of the GDPR (in the original text, Directive 95/46/EC). Alongside this provision, the PSD2 states that payment services shall only *access, process and retain* personal data necessary *for the provision of their payment services*, with the *explicit consent* of the payment service user (art. 94(2) of the PSD2, all emphases added by the author).

This means that the PSD2 provides two broad situations when personal data can be processed:

- The legal obligation to safeguard the prevention, investigation and detection of fraud (if the necessity criterion is met), thus providing the legal grounds for data processing as understood in art. 6(1)(c) of the GDPR; and
- In the absence of the first situation, with the user's explicit consent. However, it is not entirely clear if these two options are mutually exclusive.

4.2 The Curious Case of Explicit Consent

PSD2 and GDPR both recognise consent, and explicit consent, as important safe-guards of data protection. However, there are differences in how the two instruments understand the notion of consent, and the interpretations outlined here provide some useful insight into resolving the two frameworks' conflicts on ensuring data protection.

Under art. 6 of the GDPR, the data subject's consent is one of the six legal bases available to the controller to justify data processing. The data controller carries the burden of proving that valid consent has been obtained, meeting all the criteria contained in the GDPR, especially its art. 6 and 7, meaning that consent represents a freely given, specific, informed and unambiguous indication of the data subject's wishes. The GDPR also recognizes the notion of explicit consent, as legal grounds for processing of special categories of personal data (sensitive personal data). As explained in the previous section, biometric data for the purpose of uniquely identifying a natural person may well be used as the second factor in an authentication process, meaning that explicit consent under the GDPR is relevant legal grounds.

The clear division under the GDPR is muddled by the notion of explicit consent as understood by art. 94 of the PSD2. Here, explicit consent of the user

is laid out as the second option for data processing, when the first situation (legal obligations to fight fraud) is not given. Thus, the idea of explicit consent under the two instruments does not overlap. To a large extent, it was not clear if the explicit consent under art. 94(2) of the PSD2 could be considered valid legal grounds in the sense of art. 6 of the GDPR. Initially, it was argued that obtaining explicit consent might not even be necessary. The reasoning was that if the PSP could rely on other legal grounds to process personal data, such as necessary for the fulfilment of a contract between them – i.e. to provide an authentication process, and that consent should not be asked despite the PSD2's requirement [26]. Others held the view that where PSD2 requires explicit consent, the same standards for consent as required by the GDPR should be adhered to, including the information obligations towards users who are data subjects. That means that those users should be fully aware of what they are consenting to and that their data protection rights apply [6].

The dilemma was finally resolved by the EDPB in July 2020: the explicit consent as understood by the PSD2 is not legal grounds; however, it can be considered as a safeguard under data protection law as it gives the data subject the control and transparency over their personal data. In other words, explicit consent cannot be considered extra lawful grounds alongside contract performance [9].

The question of (explicit) consent has an indirect effect on authentication. Insofar as cybersecurity involves processing of personal data, the measures need to rely on valid legal grounds. If biometrics are used as the second authentication factor, then one of the valid legal bases under art. 9 of the GDPR is explicit consent.

4.3 Lex Specialis and Lex Generalis, or Cumulative Use?

There is an overlap in scopes of application of the GDPR and PSD2, when the payment service provider processes personal data. This leads us to the question of the relationship between the two instruments. The provision of art. 94 refers to processing of personal data for the purposes of the PSD2, which shall be carried out in accordance with the data protection framework, now contained in the GDPR and relevant national data protection acts. However, it does not explain any possible conflicts between the two instruments should be resolved. As explained above, explicit consent is an example of such a conflict.

One option is to explore whether the frameworks are more specific to one another, in which case the general provision must give precedence to the more specific one. The fundamental legal principle of lex specialis derogat legi generali applies in a situation when two divergent provisions are at stake; a typical example is the relationship between the GDPR and the ePrivacy regime. If the former gave greater protection than the latter, the ePrivacy regime would nevertheless apply, as it is the more specific rule [10].

However, it is unclear if that is the case here, since PSD2 explicitly refers to the data protection regime to inform the users about the processing of their data, while at the same time, the provision clarifies conditions under which

data processing can be carried out. The conditions are either that processing is necessary to safeguard the prevention, investigation and detection of payment fraud, or if the user has given its explicit consent. If both instruments regulate data processing with the aim of ensuring a high level of data protection (albeit from two different viewpoints), does that mean they are in a lex specialis and lex generalis relationship?

The position of scholars seems to be in favour of cumulative application rather than lex specialis and lex generalis relationship. Cumulative application means that both instruments apply. The reference to the application and use of GDPR is seen as an implicit need for joint application of the two – the two instruments should be read together insofar as there is an overlap in their scope of application [25]. This view has been implicitly confirmed by the EDPB in their 2020 guidelines, in which the obligations from each instrument are discussed cumulatively [9].

4.4 The Implications of Cumulative Use

How does the cumulative application of PSD2 and GDPR affect the legal regime for strong customer authentication? We provide three considerations: first, who is responsible for implementing authentication as the data controller; second, what are lawful grounds for authentication, and thirdly, what is the required security standard under either framework.

Firstly, cumulative use means that all relevant provisions of the GDPR must be complied with.

As explained above, the obligations under the GDPR centre mostly on the data controller, which is the entity determining the means and purposes of data processing. During an authentication procedure, credentials are securely processed in a pseudonymised or an encrypted form [17]. Encryption data is a form of data pseudonymisation, and pseudonymised data are considered personal data under art. 4(5) of the GDPR [8]. The decryption keys must be kept securely and separately from the identifiable personal data. Pseudonymised authentication is possible under art. 11 of the GDPR, when the purposes for which a controller processes personal data no longer require the identification of a data subject by the controller. Personalised security credentials as understood by art. 4(31) could be an example of pseudonymised authentication.

However, if a PSP only processes personalized security credentials without being able to identify the user, its position as a controller or processor is not entirely clear. In payment services, the role of controller or processor depends on the specific context [9]. In the case of encrypted data, it has long been unclear whether actual access to the decryption key is necessary to be considered a controller [23]; the question was partly answered in the Breyer case of the Court of Justice of the EU[14]. Following the reasoning of the judgment, as long as a party has the legal means which enable it to identify the data subject with additional

[14] Patrick Breyer v Bundesrepublik Deutschland. Case C-582/14. Judgment of the Court (Second Chamber) of 19 October 2016.

data, it can be considered a controller. This implies that as long as relevant decryption keys can be obtained by the PSP or other actors, the PSPs will likely be considered data controllers. Inter alia, that means that the controller carries the responsibility to comply with the GDPR's provisions, including ensuring that security measures are in place to protect the authentication related personal data.

Secondly, there must be valid legal grounds to process personal data in the course of an authentication procedure. As the EDPB explains in its Guidelines 06/2020, following its previous work, the six legal bases in art. 6 of the GDPR are listed exhaustively (para. 26). This means that authentication insofar as it represents processing of personal data must fall under one of these six options. The process of authentication has been confused with giving consent to processing of personal data; however, that is not correct [8]. Consent represents the freely given, specific, in-formed and unambiguous indication of the data subject's wish to agree to data processing (art. 4(11) of the GDPR), while authentication fulfils another goal – it ensures authorised access to and carrying out of the payment services. Therefore, other legal basis must be found.

Is there a conflict between the position of the EDPB on numerous clausus legal bases under the GDPR and the data protection clause of art. 94 of the PSD2? Recital 40 of the GDPR provides if a lawful basis is contained in a law outside the GDPR, the latter must contain a reference to the former. Therefore, we might assume that an-other law can only provide legitimisation for data processing when it further specifies one of the provisions of art. 6 of the GDPR, but other legal bases cannot exist. This would mean that while the data protection clause of the PSD2 provides for (at least) two situations in which processing of payment services-related personal data is lawful, those situations are specifications of the existing legal bases under art. 6 of the GDPR. The EDPB appears to corroborate this option in para. 35 of the Guidelines 06/2020 when it considers the position of explicit consent not to be an "additional" legal basis [11].

Drawing parallels with access to data under art. 66 and 67 of the PSD2, where PSPs can rely on necessity for a legal obligation under art. 6(1)(c) of the GDPR, it can be asked whether PSPs carry a legal obligation to process personal data to put into place cybersecurity measures, such as authentication. A similar obligation to be able to identify the signatory party can also be found in art. 26(b) of the Regulation 910/2014 (i.e. the eIDAS Regulation)[15].

The assumption of PSD2 seems to be that authentication relies on personalised credentials (art. 97(3) of the PSD2). If the credentials refer to an identifiable person, they are then considered personal data under art. 4(1) of the GDPR. However, even if credentials are not personalised (e.g. art. 11 of the GDPR allows for pseudonymous identification), the second authentication factor may well be. Biometric data, used for the purpose of uniquely identifying a natural person, are personal data according to art. 9 of the GDPR. The possession factor, such as a one-time password, might be sent to an email address or a

[15] Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market. OJ L 257.

personal mobile device. In practice, authentication largely relies on personalised credentials, since it is difficult to assess identity otherwise [17]. Nevertheless, there does not appear to be an explicit legal obligation to process personal data for authentication purposes.

The execution of the payment relies on a contractual relationship between the user and the PSP (often by means of complying with the terms of service, or terms of use), meaning that necessity for the performance of a contract may be relevant legal basis [6,26]. Alternatively, if there is no contractual relationship, for example because a third party is carrying out the authentication procedure for the PSP, legitimate interests of the PSP as the data controller may be relevant (art. 6(1)(f) of the GDPR). In this case, processing of authentication data can be carried out if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. However, the processing may not be carried out if the legitimate interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, according to art. 6(1)(f) of the GDPR. Recital 49 of the GDPR suggests that processing with the aim of ensuring cybersecurity, such as preventing unauthorised access to electronic communications networks is an example of the controller's legitimate interest. Implementing security measures, such as authentication, may therefore fall under the notion of legitimate interest.

Either legal grounds must meet the necessity requirement: data processing is lawful insofar as it is necessary, either for contractual performance or achieving legitimate interests. This may be problematic in cases of screen scraping, where the PSP may have access to more user data than is strictly necessary to carry out the payment [27], which has led to the adoption of dedicated interfaces by banks when allowing non-traditional PSPs access to user data, in accordance with art. 33(4) of the Regulatory technical standards. This means that PSPs are allowed to make use of the interfaces made available to the payment service users for the authentication and communication with their account servicing payment service provider. These interfaces will be used insofar as necessity of processing remains a concern in the context of screen scraping, according to art. 32 of the RTS.

Thirdly, authentication as a cybersecurity measure contributes to security of personal data under art. 32 of the GDPR. On principle, both the GDPR and the PSD2 require high security standards. Due to various legal requirements, the security systems may become more complex. In security design, complexity may compromise security: the more devices are involved, the more likely there will be a vulnerability [21]. Exceptions likewise contribute to complexity, since the code will need to foresee more situations [2].

However, it is difficult to say whether adopting measures to comply with the authentication requirements in art. 97 of the PSD2 and Sect. 2 of the RTS would conflict with the art. 32 of the GDPR. First argument is found in art. 18(1) of RTS, which provides for voluntary compliance with this requirement. The PSPs may, but are not obliged to implement the exceptions under their art. 18(1). Therefore, if enabling the exceptions could lead to security vulnerabilities, the PSPs may decide to use strong customer authentication for all transactions.

This might meet the standard under art. 32 of the GDPR, which requires that security of personal data must take into account the level of risk of varying likelihood and severity for the rights and freedoms of natural persons. In general, PSD2 seems to favour innovation and competition over privacy and security [18,27]; however, considering that both instruments need to be applied due to cumulative use, needing to comply with the higher cybersecurity standard may mean having to implement authentication for all payments, if compliance with art. 32 cannot be guaranteed otherwise.

5 Open Questions

This paper explored the relationship between Second payment services directive (PSD2) and the General data protection regulation (GDPR), and their cumulative application to strong customer authentication. The legal regime nevertheless leaves some open questions into which future research might provide better insight. It is also worth considering whether there is a spill over effect of strong (customer) authentication into other policy areas. The rising popularity of e-commerce in the context of the Covid-19 crisis needs a safe and secure underlying payment service infrastructure, to whose compliance the understanding of cumulative use of PSD2 and GDPR may contribute.

First, given that attack vectors multiply when several authentication procedures are used, does the access to account information under art. 66 and 67 of the PSD2 jeopardise the PSD2's stated goal of improving cybersecurity in payments? Account information service providers, and payment initiation service providers are entitled to access certain information under art. 66 and 67 of the PSD2 to perform their services. This means that three authentication procedures will be put into place: the first on the side of the bank, the second to verify the identity of the customer, and the third with the payment service provider itself. However, as Wolters and Jacobs show, this regime creates more risks, since more procedures bring the multiplication of attack vectors, which can lead to more possible vulnerabilities [27]. Does cumulative use, and the need to comply with the standard of security contained in art. 32 of the GDPR respond adequately to this problem?

Secondly, since PSD2 is a directive, it must be transposed into national legal systems by the legislative bodies of member states. Given the variety and diversity of legal systems across the EU, and various options for scope exemption in the PSD2, such as art. 2(5), allowing member states to exclude credit institutions under the capital ratings regime[16] from certain PSD2 obligations, will this lead to further conflicts for different authentication requirements in different member states, based on the type of institution providing payment services?[17]

[16] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012. OJ L 176.

[17] https://ec.europa.eu/info/files/psd2-member-states-options_en, last accessed 2020/10/16.

Thirdly, given the shift to online services, it is likely that the need for strong authentication might spill over into other policy areas. During the Covid-19 pandemic, many (public) service providers, including governments and healthcare, have been motivated to adapt to an online context. Socially distanced shopping and services usually require online banking, and stronger authentication may soon be necessary to improve cybersecurity. In that scenario, how will the cumulative use of PSD2 and GDPR interact with other frameworks, and what will be the impact on cybersecurity? For authentication purposes, PSPs could in some instances leverage the use of certificates issued under the eIDAS framework; however, the lack of legal clarity surrounding this possibility may have contributed to its slow spread [15,18,24]. Nonetheless, the shift to online services during the pandemic may be a strong incentive for private businesses to leverage the eIDAS framework, insofar as that is possible under the national law, for example in Belgium with the itsme application[18].

Finally, it remains to be seen whether the standards for strong customer authentication adopted by the PSD2 and its Regulatory technical standards become the benchmark in other policy areas when or if strong authentication requirements are mandated, or whether the legislators and the Commission will require different standards. This question can only be answered by careful examination of future regulation and policy-making at all relevant levels, from European Union and national legislation to initiatives by the industry, such as standard-setting.

References

1. Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., Upton, D.: A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate. J. Cyber Secur. **4**(1) (2018). https://doi.org/10.1093/cybsec/tyy006
2. Alenezi, M., Zarour, M.: On the Relationship between software complexity and security. ResearchGate (2020)
3. Arner, D.W., Zetzsche, D.A., Buckley, R.P., Barberis, J.N.: The identity challenge in finance: from analogue identity to digitized identification to digital KYC utilities. Eur. Bus. Organization Law Rev. **20**(1), 55–80 (2019). https://doi.org/10.1007/s40804-019-00135-1
4. European Banking Authority: Guidelines on ICT and security risk management. Technical Report. https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management
5. European Central Bank: Recommendations for the security of internet payments. Technical Report. https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpc201301en.pdf
6. European consumer organisation: Recommendations to the EDPB on the interplay between the GDPR and PSD2. Technical Report BEUC-X-2019-021 (2019). http://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf

[18] https://www.itsme.be/en/, last accessed 2020/10/16.

7. European consumer organisation and European association for the coordination of consumer representation in standardisation: Keeping consumers secure: How to tackle cyber security threats through EU law (2019). https://www.beuc.eu/publications/beuc-x-2019-066_keeping_consumers_secure_how_to_tackle_cybersecurity_threats_through_eu_law.pdf
8. European Data Protection Board: Guidelines 3/2019 on processing of personal data through video devices. Technical Report. https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-32019-processing-personal-data-through-video_en
9. European data protection board: Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR. Technical Report 06/2020 (2020). https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202006_interplaypsd2andgdpr.pdf
10. European data protection supervisor: Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation). Technical Report (2017). https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf
11. European Union Agency for Cyber security: Security of Mobile Payments and Digital Wallets. Technical Report (2016). http://www.enisa.europa.eu/publications/mobile-payments-security
12. Fuster, G.G., Jasmontaite, L.: Cybersecurity regulation in the European union: the digital, the critical and fundamental rights. In: Christen, M., Gordijn, B., Loi, M. (eds.) The Ethics of Cybersecurity. TILELT, vol. 21, pp. 97–115. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-29053-5_5
13. Hartl, V.M.I.A., Schmuntzsch, U.: Fraud protection for online banking. In: Tryfonas, T. (ed.) HAS 2016. LNCS, vol. 9750, pp. 37–47. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39381-0_4
14. Jasmontaite, L., González Fuster, G., Gutwirth, S., Wenger, F., Jaquet-Chiffelle, D.O., Schlehahn, E.: Canvas White Paper 2 - Cybersecurity and Law. SSRN Scholarly Paper ID 3091939, Social Science Research Network, Rochester, NY (2017). https://papers.ssrn.com/abstract=3091939
15. Jones, B.: Are eIDAS certificates sufficient for PSD2 Open Banking? https://www.finextra.com/blogposting/17379/are-eidas-certificates-sufficient-for-psd2-open-banking
16. Kemp, R.: Mobile payments: current and emerging regulatory and contracting issues. Comput. Law Secur. Rev. **29**(2), 175–179 (2013). https://doi.org/10.1016/j.clsr.2013.01.009, http://www.sciencedirect.com/science/article/pii/S0267364913000277
17. Kogetsu, A., Ogishima, S., Kato, K.: Authentication of patients and participants in health information exchange and consent for medical research: a key step for privacy protection, respect for autonomy, and trustworthiness. Front. Genetics **9** (2018). https://doi.org/10.3389/fgene.2018.00167. https://www.frontiersin.org/articles/10.3389/fgene.2018.00167/full
18. Mansfield-Devine, S.: Open banking: opportunity and danger. Comput. Fraud Secur. **2016**(10), 8–13 (2016). https://doi.org/10.1016/S1361-3723(16)30080-X. http://www.sciencedirect.com/science/article/pii/S136137231630080X
19. Passi, L.F.: An open banking ecosystem to survive the revised payment services directive: connecting international banks and FinTechs with the CBI globe platform. J. Payments Strategy Syst. **12**(4), 335–345 (2018). http://kuleuven.ezproxy.kuleuven.be/login?url=https://www.dynamed.com

20. Rousseau, H.P.: GDPR, PSD2 and open banking are creating a new dynamic in personal financial services: a note - ProQuest. J. Internet Bank. Commer. 24(1), 1–7 (2019). http://search.proquest.com/docview/2278751804?rfr_id=infonumber:1
21. Schneier, B.: News: Complexity the Worst Enemy of Security - Schneier on Security (2012). https://www.schneier.com/news/archives/2012/12/complexity_the_worst.html
22. Schneier, B.: Stop trying to fix the user. IEEE Secur. Privacy **14**(5), 96 (2016). https://doi.org/10.1109/MSP.2016.101
23. Spindler, G., Schmechel, P.: Personal data and encryption in the European general data protection regulation. JIPITEC **7**(2) (2016). http://www.jipitec.eu/issues/jipitec-7-2-2016/4440
24. Terziman, L.: The eIDAS Challenge for TPPs under PSD2. https://www.finextra.com/blogposting/17221/the-eidas-challenge-for-tpps-under-psd2
25. Thys, T., Van Raemdonck, S., Desmet, K.: GDPR, PSD2 and the repurposing of data: no big deal? Droit bancaire et financier - Bank- en Financieel Recht **2018**(3), 144–197 (2018), https://www-jurisquare-be.kuleuven.ezproxy.kuleuven.be/en/journal/bfr/2018-3/financiele-reglementering-actualiteit-il-est-urgent-dattendre-bedenkingen-bij-het-fintech-action-pla/index.html#page/144/search/
26. Vandezande, N.: Reconciling Consent in PSD2 and GDPR (2020). https://thepaypers.com/expert-opinion/reconciling-consent-in-psd2-and-gdpr-777976
27. Wolters, P.T.J., Jacobs, B.P.F.: The security of access to accounts under the PSD2. Comput. Law Secur. Rev. **35**(1), 29–41 (2019). https://doi.org/10.1016/j.clsr.2018.10.005, http://www.sciencedirect.com/science/article/pii/S0267364918302620
28. Yaghmaei, E., et al.: Canvas White Paper 1 - Cybersecurity and Ethics. SSRN Scholarly Paper ID 3091909, Social Science Research Network, Rochester, NY (2017). https://papers.ssrn.com/abstract=3091909, issue: ID 3091909