Main Document – Anonymous

INCOMPATIBILITY OF FINANCIAL BLOCKING MEASURES AGAINST GAMBLING OPERATORS WITH DATA PROTECTION LAW

Using Banks to Control Citizens.

Original Article

Key Points

- Financial Blocking measures are almost as severe as the general data retention by telecommunication services – this time in the banking sector. As such, they pose a threat to the right to privacy, protected by Articles 7 and the right to data protection, protected by Article 8 of the Charter of Fundamental Rights of the European Union as well as the EU-General Data Protection Regulation 2016/679 (GDPR).
- Member States have the exclusive competence in the field of gambling and defend their monopolies in the internal market against EU law. However, since the partial opening of the Internet as a sales channel in 2012, German gambling supervisory authorities face increasing difficulties with the enforcement of the German Inter-State Treaty on games of chance (GlüStV), which provides them with various instruments to combat unlawful games of chance.
- Aside from prohibitory orders against unlawful gambling operators, national gambling authorities may issue orders against banks in order to prevent payments connected with unlawful gambling (Financial Blocking).
- Such orders against gambling operators and players require the processing of personal data on a massive scale, encompassing the data of all bank customers. The GlüStV lacks a clear and precise legal basis as required under data protection law on how such Financial Blocking measures are supposed to be enforced or what form they should take.
- This Article analyses the compatibility of German Financial Blocking provisions in the light of EU data protection law. The findings apply equally to other Member States. As many EU Member States already apply or plan to introduce similar measures in order to enforce their respective national gambling monopolies, Financial Blocking constitutes a threat to privacy in the EU as a whole.

Keywords

Bank Data

Consent

Data Retention

Online Gambling

Payment Blocking

Prohibition on Games of Chance

I. Introduction

The age of digitalization is both a curse and a blessing at the same time. While it improves international mobility, global communication and exchange of information, it also increases governments' surveillance abilities. From a technical view, the comprehensive interception of telecommunications and monitoring of bank accounts may seem tempting for governments. States have long been introducing and expanding surveillance measures to protect important legal interests in the fight against terrorism and organised crime. However, the threshold has been lowered from time to time and far-reaching surveillance measures are introduced for minor crimes and to avert danger in general. Germany and many other EU Member States allow the monitoring of bank accounts in order to prevent the participation in and operation of unlawful games of chance ('Financial Blocking'). This essay outlines the limits set by the high standard of the new EU Data Protection Framework to Financial Blocking. It also highlights the legal limitations when States charge entities of the private sector (banks, telecommunication companies, etc.) with the implementation of surveillance measures in the public interest. After this introduction, the section 'Overview of the Legal Framework on Gambling Law' provides information on EU Law and on the legal basis for Financial Blocking in German Law. The section 'The Applicable data protection law' will outline the relevant legal framework, which is now governed by the EU-General Data Protection Regulation 2016/679 (GDPR) and complementary national legislation, the German Federal Data Protection Act (BDSG). The core of this article is the following section assessing the 'Lawfulness of collecting additional data under the GDPR' in more detail. The section 'Using existing data for another purpose' will deal with the question of whether data that have already been retained for the purpose of combatting money laundering and terrorist financing could now be reused for the prevention of unlawful games of chance. Finally, the section 'Outlook' will show that as Financial Blocking measures exist in many EU-Member States, the issue discussed in this article is of relevance for the EU as a whole.

II. Overview of the legal framework on gambling law

This Section first provides an overview over gambling regulation in the EU and the Member States, with a particular view on Germany. It will also provide background information on which entities Financial Blocking measures apply. The last Subsection deals with questions surrounding the technical realization of Financial Blocking orders.

1. EU Law

Due to the absence of Community harmonisation, legislation on gambling is one of the few areas in which Member States are free to define their own level of protection. However, they must observe the fundamental rules of the Treaties, in particular the principles of equal treatment and non-discrimination on grounds of nationality. EU law sets limits for national gambling legislation. Not only does the internal market offer a space for operators and players of games of chance to meet outside the realm of national regulations, but it also sets a standard that many national regulations of Member States have failed to achieve. The European Court of Justice (CJEU) has repeatedly ruled on German gambling regulation and abolished disproportionate restrictions of Articles 49 and 56 of the TFEU whilst applying a strict consistency test.[1] This article will discuss Financial Blocking measures, as provided for under German gambling law. Such measures restrict the right to free movement of payments of the banks, operators of games of chances and players as well as the freedom to provide services and probably even the free movement of capital provided for under Article 63(1) of the TFEU. However, this essay will not deal with the possible contravention of fundamental freedoms. It rather focusses on the compatibility of Financial Blocking orders with data protection law.

2. Legal Basis for Financial Blocking Measures

Under German Law, legislation on games of chance falls primarily within the competence of the *Länder*. To coordinate the divergent rules on gambling, the 16 *Länder*[2] adopted an Inter-State Treaty on games of chance ('Glücksspielstaatsvertrag' or 'GlüStV'). In reaction to several CJEU-judgments and in an attempt to liberalise the law on games of chance, the Inter-State Treaty was amended and ratified in 2012 by 15 *Länder,* the *Land* Schleswig-Holstein adopted it in 2013.[3] The GlüStV applies to all games of chance, in particular to lotteries, casino games, sports and horse race betting, poker and in part also to slot machine gambling. The 16 *Länder* have a monopoly on the operation of lotteries. Licences for land-based casinos, gambling machines, sports and horse race betting are granted in limited number

[1] See case C-336/14 *Ince* [2016] ECLI:EU:C:2016:72 and BVerwGE 155, 261; case C-156/13 *Digibet and Albers* [2014] ECLI:EU:C:2014:1756; case C-46/08 *Carmen Media Group* [2010] ECLI:EU:C:2010:505.

[2] The Federal Republic of Germany consists of 16 federal „States". In German, they are referred to as 'Länder' in the plural and 'Land' in the singular. The German term is also used in the official English version of the German constitution, the Basic Law, as it describes German Federalism more precisely.

[3] Between 1 January 2012 and 8 February 2013, the *Land* Schleswig-Holstein was not party of the GlüStV and had its own gambling law. During this period, it granted licenses for online casinos and sports betting operators that remain valid.

under the new GlüStV. Section 4(1) GlüStV generally prohibits the organisation or intermediation of public games of chance without authorisation of the competent *Land* authority. Regarding online gambling, the GlüStV is stricter and imposes a general prohibition on the organisation and intermediation of online public games of chance in section 4(4). Due to the liberalisation in 2012, online lotteries and sporting bets may be authorised by the *Länder* under strict conditions, whereas online casinos are banned completely. Section 4(1) GlüStV prohibits banks and financial institutions to participate in payments related to unlawful gambling. In order to enforce this additional prohibition, section 9(1) no. 4 of the GlüStV provides a legal basis to ban banks and financial services institutions from processing payments related to the participation in and offering of unlawful games of chance. The measure may only be applied "after prior notification" to the banks of unlawful gambling activities. Measures under section 9(1) no. 4 GlüStV are referred to as Financial blocking. The operation of unauthorised games of chance as well as the participation in such games also constitute a criminal offence under the german criminal law. As primary prohibition orders against illegal gambling operators outside the German territorial jurisdiction are difficult to enforce, the authorities aim at intermediary banks and financial services located in Germany to prevent unlawful gambling.

3. Addressees of Financial blocking orders

It is still unclear how the supervisory authorities shall enforce Financial Blocking measures and which entities they should address.[4] The authorities' options range from "orders on a case-by-case basis" (section 9(1), second sentence of the GlüStV) in the form of specific, individual prohibitions of participation (by force of an official order) to informal "agreements" made with payment services providers.[5] Other options discussed are e.g. publishing lists of unauthorized offers by operators of games of chance ('blacklisting method'[6]) or providing banks, financial services institutions and payment services providers with internal "dossiers".[7] These institutions would then be obliged to block payment

[4] Generally shared view, see C Hambach and B Brenner, in R Streinz, M Liesching and W Hambach (eds), *Glücks- und Gewinnspielrecht in den Medien* (CH Beck 2014) s 9 GlüStV para. 81.

[5] For more detail see Lower Saxony State Parliament Document (LT-Drs.) 17/3683, 2.

[6] Initially the German Federal Government favoured this approach in its Communication to the Commission of 20 May 2008, infringement procedure no. 2007/4866, Zeitschrift für Wett- und Glücksspielrecht (ZfWG) [2008], 173; now taking a different approach: German Parliament Document (BT-Drs.) 17/10745, 17 (right column); see also M Steegmann, *Die Haftung der Basisinfrastruktur bei rechtswidrigen Internetangeboten* (Nomos 2010) 214; C Brugger, *Abbruch der Zahlungsströme als Mittel zur Bekämpfung unerlaubter Internetglücksspiele* (Peter Lang 2012) 163; J Hilf and K Umbach, in F Becker, J Hilf, N Nolte and D Uwer (eds), *Glücksspielregulierung* (Carl Heymanns 2017) s 9 GlüStV para. 53.

[7] C Koenig, 'Einbindung des Glücksspielkollegiums in die ordnungsrechtlichen Sanktionsverfahren der Länder' [2016] ZfWG 2, 4 referring to insider information.

transactions on a case-by-case basis.[8] State authorities further consider encouraging banks to include special clauses into their standard terms and conditions in order to ensure that credit cards are only used for authorised online games of chance.[9] These proposed instruments have in common that all parties involved in the payment processes can be subjected to obligations indiscriminately. Credit institutions and financial services providers[10] are the first and foremost addressees of Financial Blocking measures, as are payment services providers and payment institutions, including electronic money institutions, offering non-cash payments. The gambling supervisory authority may issue blocking orders under section 9(1) no. 4 of the GlüStV targeting the bank deposits of players as well as of operators of games of chance alike.

4. Technical Realization

Depending on the specific mode of payment, different technical means to effectuate Financial Blocking are possible:[11] for instance, payments related to unlawful gambling could be identified and blocked on the basis of the Merchant Category Code (MCC) 7995.[12] However, the MCC does not reveal whether the particular offer of game of chance in question is lawful or not.[13] If the method of blacklisting is adopted, the gambling supervisory authorities will have to list unlawful operators of games of chance and the banks involved in the payment processes would merely have to block payments by or to the listed operators.[14] Payments for unlawful games of chance via money transfer could be blocked if unlawful transactions were to be identified as such on the basis of certain keywords in the reason for payment on the bank transfer slip.[15]

[8] cf Lower Saxony State Parliament Document (LT-Drs.) 17/3683, 3.
[9] C Koenig and A Jäger, 'EU-rechtskonforme Optionen zur Neuordnung der Regulierung der (digitalen) Glücksspielwirtschaft in Deutschland' [2016] ZfWG 286, 288 referring to insider information.
[10] Explanatory memorandum on the GlüStV, Bavarian State Parliament Document (LT-Drs.) 16/11995, 27.
[11] For further possibilities see Baden-Württemberg State Parliament Document (LT-Drs.) 15/1707, 11–12; since the amendment of the German Anti-Money Laundering Act ("GwG") in 2017 online gambling transactions may only be effected by direct debit, a bank transfer or by means of a payment card issued with the gambler's name, s 16(4) GwG. However, this does not apply to terrestrial propositions and transactions on the non-regulated market that accounts for a market share of approx. 80% in the online sector, cf. annual report by the Lands' supervisory authorities, 'Jahresreport der Glücksspielaufsichtsbehörden der Länder', 23 November 2016, 13.
[12] For more detail see Brugger (n 6) 155ff. and at 233.
[13] The creation of a Uniform Code for online gambling provided for under s 9d GwG (old version), was never realised and is no longer provided for in the new version of the GwG.
[14] Meanwhile clearly rejecting the use of such lists: German Parliament Document (BT-Drs.) 17/10745, 17.
[15] W Hambach, 'Aktuelle Entwicklungen im Online-Glücksspielrecht: Keine Ruhe für den GlüStV' [2014] Kommunikation & Recht 570, 576.

III. THE APPLICABLE DATA PROTECTION LAW

Financial blocking measures require the processing of significant amounts of personal data. Therefore, data protection law – a field of law that previously was widely unrecognized in gambling law – comes into play as a test of legality. Before dealing with the legality of the processing in detail, this Section explains the applicability of the GDPR in conjunction with the BDSG as a legal test.

1. Applicability of the GDPR

There is no specific legal basis in German gambling law allowing banks to collect such data or supervisory authorities to transmit the necessary data to the payment institutions. Likewise, the parties involved in the payment transactions are under no general obligation to transmit stored bank customer data to the supervisory authority for the purpose of preventing unlawful games of chance.[16] Therefore, the relevant data protection regime for the legal assessment of Financial Blocking measures is the GDPR.

Financial Blocking is covered by the material scope of the GDPR as defined Article 2(2) of the GDPR. In particular, Financial Blocking is not an activity in the area of national safety (Article 2(2)(a) of the GDPR) and does not constitute processing of personal data for the purposes of criminal prosecution (Article 2(2)(d) of the GDPR). The latter exception only applies to the processing of data directly by the competent national law-enforcement authorities and not to the processing of data by private bodies even if they engage in field of prevention of threats to public security.[17] Financial blocking requires non-public bodies to process data, making use of their customer knowledge. If private entities, governed by private law, are entrusted with public tasks in the public interest as part of the services they provide (and which are protected by the fundamental rights), the GDPR is applicable regardless of whether national authorities access these data at a later stage for the purposes of national security or the prevention of crime.

[16] The new Anti-Money Laundering Act that entered into force on 26 June 2017 contains a provision in s 51(7) GWG 2017 allowing gambling supervisory authorities to collect information from banks and payment institutions about payment processes of online gambling providers or agents and of players. However, this does not constitute a general data transfer obligation of the banks, but rather is limited to providing information "in individual cases" only and upon request.

[17] cf joint cases C-203/15 *Tele2 Sverige v Post-och telestyrelsen* and C-698/15 *Secretary of State for the Home Department v Tom Watson* [2016] ECLI:EU:C:2016:970, paras. 73–81; see also recital 19 of the GDPR.

2. BDSG as Relevant Test of Legality

However, data processing for the purpose of combating unlawful games of chance is not governed by the GDPR alone as it falls within the scope of the opening clauses in Article 6(1)(c) and (e) in conjunction with Article 6(3) of the GDPR. These opening clauses are complemented on a national level by the BDSG, which therefore constitutes a supplementary test of legality. This is all the more so, as gambling law is in a non-harmonised area in which, according to the CJEU, "there are significant moral, religious and cultural differences between the Member States"[18] and the Member States are therefore entitled to exercise a wide measure of discretion.

This is not only relevant for the level of regulation, but also has an impact on the relevant regime of fundamental rights. As the provisions of the GlüStV do not serve to implement EU law, it is not compulsory to solely apply the EU Charter of Fundamental Rights (EU Charter) as the relevant test of legality when assessing the proportionality. Vice versa, the (parallel) application of national fundamental rights is not excluded because of Article 51(1) of the EU Charter. After all, in the matter at hand, both systems of fundamental rights offer the same level of protection, allowing this essay to focus only on to the EU Charter.

IV. Lawfulness of collecting additional data under the GDPR

At the core of this analysis lies the question of legality under the GDPR and the BDSG that will be answered in this Section. Both, collecting personal data and transmitting them to the competent gambling supervisory authorities are data processing operations in the sense of Article 4(2) of the GDPR that have to meet certain conditions laid down in Article 6 of the GDPR in order to be considered lawful. According to this provision, the processing of personal data is only allowed, if one of the six grounds that are mentioned in Article 6(1) of the GDPR is met. These conditions are conclusive and must be fulfilled at the time of the processing of data.

Subsection 'Additional personal data needed' will first give an overview over the personal data that is need by the banks and financial services providers to enforce Financial Blocking. Under Subsection 'Lack of prior consent' the possibility of consenting into surveillance measures according to Article 6(1)(a) of the GDPR will be discussed. The following Subsections deal with the compatibility of monitoring payment transactions with Article

[18] This constitutes settled case-law, see recent judgment in case C-463/13 *Stanley International Betting and Stanleybet Malta* [2015] ECLI:EU:C:2015:25, para. 51 with further ref.

6(1)(b)-(f) of the GDPR in the light of the fundamental right provision of Articles 8(1), 52(1) of the EU Charter prohibiting disproportionate retention measures.

1. Additional personal data needed

In order to assess whether a financial transaction is linked to unlawful games of chance, the banks have to collect additional personal data, beyond the data already processed in the course of their usual business, i.e. to perform duties within contractual relationships or to fulfil their legal obligations.[19] Banks will need additional personal data on the specific purpose of the payment (regardless of the amount transferred), as operators of games of chance naturally do not only receive payments from their players. To find out if the participation in games of chance is unlawful, they need further personal data on the participants of unlawful games of chance, in particular their age and their location[20] at the time of gambling. The use of localisation technology to determine the player's location at the time of online gambling further requires – in the case of games of chance on the internet – tracing the IP-address and the related location data. It must also be known whether the operator holds a German licence, of the validity of the licence and of which *Land* has issued the licence.[21] In order to conduct effective Financial Blocking, banks would thus have to feed their existing monitoring systems with a significant amount of additional data on operators and players alike.

The starting point for assessing whether collecting such data is lawful under data protection law is the general prohibition on the processing of data provided for in Article 6 of the GDPR. According to this provision, the processing of personal data is only allowed, if one of the six grounds that are mentioned in Article 6(1) of the GDPR is met. These conditions are conclusive and must be fulfilled at the time of the processing of data.

2. Lack of Prior Consent

In the case of Financial Blocking, unambiguous consent of the data subjects as required under data protection law, cannot be assumed. The data subjects have not given their express consent according to Article 6(1)(a) in conjunction with Article 7 of the GDPR. Consent can

[19] cf W Spoerr, 'Finanzwesen' in H A Wolff and S Brink (eds) *BeckOK Datenschutzrecht* (22nd edn, CH Beck 2017) para. 137.

[20] The State Government of Lower Saxony denies this requirement, albeit without providing any explanations as to how Payment Blocking can work without geo-localisation and monitoring, document (LT-Drs.) 17/3683, 2, answer to question 1.

[21] Opinion of the Independent Centre for Data Protection of the Land Schleswig-Holstein (DPO SH) [2015] ZfWG 121, 122. For further data categories required, see Hambach (n 15) 576.

also not be obtained if the customers have to agree to the use of their personal data for Financial Blocking in the banks' standard terms and conditions. In order to be valid, recital 32 of the GDPR states, that consent "should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her". While the standard terms and conditions of banks may possibly be worded in an "intelligible and easily accessible form", as required under Article 7(2) of the GDPR and satisfy the principle of transparency, consent will most likely not be given freely und thus not be valid under Article 4(11) and Article 7(4) of the GDPR. It will also lack the specific purpose as required under Article 6(1)(a) of the GDPR.

According to the prohibition of conditionality laid down in Article 7(4) of the GDPR, account shall be taken of whether the performance of a contract is conditional on consent on the processing of personal data that is not necessary for the performance of that contract in order to assess whether consent is a free decision. Doubts arise, when the data subject is in a situation of financial distress or imbalance and when reasonably acceptable alternatives for the desired service are unavailable on the market. Under such circumstances, the data subject rarely has a "genuine or free choice"[22] as refusing consent would cause him or her huge detriment. A clause that obliges bank customers to agree to constant surveillance of their payment flows for the purpose of Financial Blocking against gambling operators as a condition to banking services, will be "practically not negotiable"[23] taking into account the contractual imbalance and the customer's existential dependency on the banks' services.

In addition, consent must be unambiguously given for each single data processing phase (as defined in Article 4(2) of the GDPR) and for all processing purposes.[24] The clause must specify business purposes as well as the type of data needed for Financial Blocking. Standard terms and conditions must include clauses that expressly mention the collection and potential transmission of the personal data to the competent gambling authority. The principle of legal certainty requires a higher level of precision the more sensitive the personal data concerned is,

[22] Recital 42 Sentence 4 of the GDPR; G Ziegenhorn and K v Heckel, 'Datenverarbeitung durch Private nach der europäischen Datenschutzreform. Auswirkungen der Datenschutz-Grundverordnung auf die materielle Rechtmäßigkeit der Verarbeitung personenbezogener Daten' [2016] Neue Zeitschrift für Verwaltungsrecht (NVwZ) 1585, at 1587.

[23] See the ruling in a case concerning insurance contracts of the BVerfG (German Federal Constitutional Court) NJW 2013, 3086; BVerfG MMR 2007, 93; also BGH (German Federal Court of Justice) MMR 2010, 138, 139; BGH MMR 2008, 731, 733.

[24] See Recital 32 sentence 4 of the GDPR; HJ Schaffland and G Holthaus, in HJ Schaffland and N Wiltfang (eds), *BDSG/DSGVO Kommentar* (issue 3/17, Erich Schmidt 2018) art 7 DSGVO para. 44; S Schulz, in P Gola (ed), *DSGVO Kommentar* (CH Beck 2017) art 6 para. 22.

the more uncommon data processing is in the respective contractual relationship and the less it is related to the actual business purpose.[25] Therefore, from a legal point of view, it is rather impossible to specify the purposes and each processing phase with the required degree of accuracy in a general clause of the standard terms and conditions. If this was seen less strictly, public entities would be able to bypass the privacy requirements laid down in Article 6(1)(e) of the GDPR by demanding standard terms and conditions in which private purposes are tied to public purposes. However, engaging private entities to carry out tasks in the public interest shall not lead to the lowering of data protection standards.

3. Not Necessary for the Performance of a Contract

Collecting additional data to identify payments made for unlawful games of chance is not necessary to duly perform the duties of the bank-customer-relationship and therefore no lawful processing in the sense of Article 6(1)(b) of the GDPR. The admissible purposes are defined in the contract between the customer and his bank. In the relevant contractual relationship between the player and his payment service provider (issuer), the latter is primarily obliged to execute a payment transaction for the payment service user (i.e. the player), which is to transfer an amount of money, regardless of the underlying legal relationship between the payer and the payee.[26] As regards the contractual relationship between the operator of games of chance and his payment service provider (acquirer), the latter's contractual obligation is to carry out payment processes.[27] Within these contractual relationships, only data that serves to carry out the cardholder's payment transactions and to maintain the payment account is considered necessary. This does not include personal data on the underlying legal relationship between the bank customer and his payee.[28]

Moreover, collecting additional data is not necessary to establish or maintain a (contractual) relationship of trust between the bank customer and the bank.[29] Contrary to crime prevention at the expense and for the account of the banks,[30] the fight against (unlawful) games of chance

[25] cf Schaffland and Wiltfang (n 24) s 4a BDSG para. 19; Opinion 1/15 *Accord PNR UE-Canada* [2017] ECLI:EU:C:2016:656, para 155-163.
[26] C Walz, in J Ellenberger, M Findeisen and G Nobbe (eds), *Kommentar zum Zahlungsverkehrsrecht* (22nd edn, Finanz Colloquium 2014) s 675f BGB para. 25.
[27] Ibid, para. 26.
[28] See also Die Deutsche Kreditwirtschaft, *Stellungnahme zum Regierungsentwurf eines Gesetzes zur Ergänzung des Geldwäschegesetzes*, 28 August 2012 (on s 9d GwG old version) 3–4.
[29] For the duties, see KJ Hopt and M Roth, in H Schimansky, HJ Bunte and HJ Lwowski (eds), *Bankrechts-Handbuch* (5th edn, CH Beck 2017) s 1 para. 1ff.
[30] Qualifying this as an economic self-interest of banks: Spoerr (n 19) para. 141; disagreeing: F Herzog, 'Der Banker als Fahnder? Von der Verdachtsanzeige zur systematischen Verdachtsgewinnung - Entwicklungstendenzen der Geldwäschebekämpfung' [1996] Zeitschrift für Wirtschafts- und Bankenrecht

is not carried out in the banks' interest. Credit institutions do not have a contractual right to analyse the payment data and monitor their clients for other reasons than for assessing their creditworthiness or preventing fraud.[31] However, criminal law considers neutral acts that are typical in the trade, such as providing bank accounts and executing transfer orders to be socially acceptable, they are therefore – in general – not punishable by law.[32]

4. Not Necessary for Compliance with a Legal Obligation

The processing for the purpose of Financial Blocking measures may however be considered necessary for compliance with a legal obligation to which the credit and payment institutions are subject within Article 6(1)(c) of the GDPR. According to Article 6(3) of the GDPR, the legal basis for the processing under point (c) containing the legal obligations on private entities, shall be laid down by Member State law and meet certain requirements of rule of law. The provisions of the GlüStV do not meet these requirements.

a. Not sufficiently precise

The legal basis as required under Article 6(3) of the GDPR must comply with Articles 8(2), 52(1) and Article 52(3) of the EU Charter.[33] Although these provisions do not necessarily require a legislative act adopted by a parliament, they nevertheless demand the legal basis to be "by force of objective law".[34] National legislation must lay down clear and precise rules governing the scope and application of Financial Blocking measures in order to be foreseeable to the persons subjected to it and to ensure that the measure is limited to what is strictly necessary.[35] The more serious and far-reaching the interference with fundamental rights is, the higher the required level of precision and limitation of purpose of the measure[36]

(WM) 1753, at 1758 according to whom anti-money laundering measures are a genuine State task and the banks' interest therein is a mere 'reflex'.

[31] KU Plath in KU Plath (ed), *BDSG/DSGVO Kommentar* (2nd edn, Verlag Dr. Otto Schmidt 2016) art 7 DSGVO, s 28 BDSG para. 95.

[32] JP Rock and C Kaiser, *Kontrolle der Finanzströme* (2nd edn 2011) 25ff; JP Rock and M Seifert, 'Abwicklung von Kreditkartenzahlungen für unerlaubtes Glücksspiel – ein Fall strafbarer Geldwäsche?' [2009] Zeitschrift für Bankrecht und Bankwirtschaft (ZBB) 377; M Hecker and M Steegmann, 'Zur Mithaftung von Kreditinstituten und sonstigen Teilnehmern am illegalen Glücksspiel (gem. §§ 284, 287 StGB)' [2006] Zeitschrift für Wettbewerb in Recht und Praxis (WRP) 1293, 1296; see for a more differentiated approach: B Berberich and H Kudlich, 'Zahlungsdienstleistungen im Zusammenhang mit Glücksspiel-Angeboten im Internet als Geldwäsche?' [2016] ZfWG 179.

[33] See eg case C-468/10 *ASNEF* [2011] ECLI:EU:C:2011:777, para. 42; Joint cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others* [2014] ECLI:EU:C:2014:238, paras. 46, 69.

[34] This view was very early shared by U Dammann and S Simitis, *EG-Datenschutzrichtlinie* (Nomos Verlag 1996) art 7 para. 7; S Ernst, in B Paal and D Pauly (eds), *Datenschutz-Grundverordnung/ Bundesdatenschutzgesetz* (2nd edn, CH Beck 2018) art 6 para. 36.

[35] Recital 41 of the GDPR; *Digital Rights Ireland* (n 33) para. 54; *Tele2 Sverige* (n 17) para. 109.

[36] See *PNR UE-Canada* (n 25) para 182-5; arguing in favour of increased clarity requirements for measures imposing payment blocking: VGH Mannheim (Higher Administrative Court of Baden-Württemberg) ZfWG

– and the less processing can be assumed to simply be "tacitly" included in the respective legal provision defining a public task.[37] The competent authority for processing the relevant data must also be specified in the law. The general obligations arising from section 4(1) GlüStV, and its specification in section 9(1) no. 4 GlüStV, do not satisfy the above mentioned requirements. It is already unclear which entity or competent state authority will be entrusted with the task to collect the necessary additional data: it could be the (private) parties directly involved in the payment process or the competent authority. However, due to the federal structure, enforcement of gambling is a matter of each of the 16 *Länder.* As an exception to this, section 9a(2) of the GlüStV stipulates that if games of chance are offered in more than one *Land*, the competent authority for measures under section 9(1) no. 4 of the GlüStV is the supervisory authority of the Land Lower Saxony. It is unclear, which of the *Land* authorities is competent for Financial Blocking orders. Also, section 9(1) no. 4 of the GlüStV grants the executing authority considerable margin for discretion with regard to the contents of the official order issued. It makes no mention of the relevant data categories, of how they should be collected and of which are the data subjects concerned (player and/or operator) to reliably filter the unlawful transactions. It thus only qualifies as a provision allocating a general task with indeterminate content – it does not satisfy the requirements for a legal basis under Article 6(3) of the GDPR.

b. Proportionality

Aside from the lack of clarity of the legal basis, data processing can further not be considered "necessary" for the purpose of the interests pursued (enforcement of the GlüStV) as required under Article 6(1)(c) of the GDPR. According to the concept of necessity as laid down in Article 6(1)(c) of the GDPR, which has its own independent meaning in EU law, it has to be ensured that the purpose of the objectives pursued does not disproportionately interfere with the fundamental rights of the data subjects.[38] Interferences with the fundamental rights arising from Articles 7 and 8 of the EU Charter must be "limited to what is strictly necessary" according to Art. 52(1) of the EU Charter.[39] This implies a particularly strict proportionality

2016, 50, para. 23; dissenting: OVG Lüneburg (Higher Administrative Court of Lower Saxony) ZfWG 2016, 451, para. 11.

[37] P Gola, C Klug and B Körffer, in P Gola and R Schomerus (eds), *BDSG Kommentar* (12th edn, CH Beck 2015) s 4, para. 7ff; Schulz (n. 24), para. 174; H Jarass, in H Jarass and B Pieroth (eds), *Grundgesetz Kommentar* (14th edn, CH Beck 2016) art 2 para. 58ff; see to the contrary, the Opinion of the DPO of the *Land* Schleswig Holstein, considering the GlüStV to be sufficiently precise (n. 21) at 123.

[38] Case C-524/06 *Huber* [2008] ECLI:EU:C:2008:724, para. 52; case C-465/00 *Österreichischer Rundfunk u.a.* [2003] ECLI:EU:C:2003:294, para. 83.

[39] cf *Digital Rights Ireland* (n 33) paras. 34ff on providers of electronic communication services.

test.[40] However, the debate about what really are the GlüStV's objectives and whether they are legitimate shall not be opened up here.[41] For the following analysis, it shall rather be assumed that the objectives stated, in particular combating addiction to gambling and ensuring the protection of minors and players, are legitimate objectives and are in principle capable of justifying restrictions of fundamental rights.

aa. Lacking Appropriateness of Financial Blocking Measures

Financial blocking is at first not a suitable measure to prevent unlawful games of chance.

From a technical point of view, financial institutions and payment services providers usually do not have the means to identify payments related to unlawful games of chance in the fully automated mass payment business with absolute certainty,[42] especially considering the divergent legal regimes in the Member States, which are subject to constant changes.

Even if banks were provided with black- or whitelists by the authorities, such lists would still not suffice to clarify whether participating in gambling in a particular case was lawful or not. For instance, a gambling operator may hold a licence in his *Land*, but act against this licence by offering gambling in another *Land*. Alternatively, it may be possible, that a player lawfully participates in a game of chance that is prohibited in his *Land* simply by crossing the border. The transaction will then be considered legal, as the relevant point of reference for judging the legality is the location of the player at the time of gambling and not at the time of the payment execution. With the existing customer and payment data alone, banks cannot sufficiently evaluate the legality of a transaction.

This uncertainty also remains, when payments are made via credit card. The MCC issued by the credit card acceptance office is uniform for unlawful and lawful games of chance.[43] Therefore, it is impossible to determine by reference to the MCC whether the operator holds a

[40] Case C-73/07 *Satakunnan Markkinapörssi und Satamedia* [2008] ECLI:EU:C:2008:727, para. 56; *Digital Rights Ireland* (n 33) para. 52; *Tele2 Sverige* (n 17) para. 94, with a case note by A Sandhu, 'Die Tele2-Entscheidung des EuGH zur Vorratsdatenspeicherung in den Mitgliedstaaten und ihre Auswirkungen auf die Rechtslage in Deutschland und in der Europäischen Union' [2017] Zeitschrift Europarecht (EuR) 453, at 459.

[41] cf on the discrepancy between the objectives prescribed and those actually pursued D Uwer, 'Die unwahre Gesetzesbegründung' in C Franzius et al. (eds), *Beharren. Bewegen., Festschrift Kloepfer* (Duncker & Humblot 2013) 867ff.

[42] See also Hambach and Brenner (n 4) s 9 GlüStV para. 60; Bolay and Pfütze in R Streinz, M Liesching and W Hambach (eds), *Glücks- und Gewinnspielrecht in den Medien* (CH Beck 2014), s 4 GlüStV para. 51; Rock and Kaiser (n 32) 82.

[43] cf Baden-Württemberg State Parliament Document (LT-Drs.) 15/1707, 11; Rock and Kaiser (n 32) 77ff.

licence and whether the specific offer in question is covered by it. The legality of the specific gambling offer can also not be determined by reference to the gambling company alone.[44]

There are more reasons that lead to the conclusion that Financial Blocking measures are inappropriate. For instance, there will be several methods, especially alternative payment channels, which allow for anonymous payment. Whilst this may limit the effectiveness of the measure in question, it does not however, make it possible to regard Financial Blocking as per se totally inappropriate for achieving the objectives pursued.[45] A measure does not need to be "wholly reliable"[46] in order to be considered appropriate. On the other hand, the measure must not be wholly inappropriate either. One must bear in mind that Financial Blocking can only be successful if the providers on the unregulated (grey) market use accounts with domestic banks. This is, because in practice, blocking orders under section 9 (1) no. 4 of the GlüStV are primarily intended to be enforced against domestic banks and their branches.[47] The providers of unlawful games of chance, however, mainly maintain bank accounts abroad and even process payments through payment services providers, financial institutions, and banks that are resident in non-EU countries.[48] Especially in the field of online payment services, numerous service providers operate outside the territorial jurisdiction of the German government, as is the case with online gambling companies. If the payment institution is just as out of reach, as the primary operator of unlawful games of chance, there is no need to resort to the former. Rather, it can be anticipated that in the field of payment processing, too, there will be an exodus to the illegal market.[49]

bb. Lack of Necessity

Secondly, Financial Blocking orders are not necessary, as there are less intrusive but equally appropriate measures. Unlawful online gambling activities can be tracked much easier and more effectively so that it is unnecessary to take additional recourse to the parties involved in the payment process.[50] This is even more so considering that the additional obligations are

[44] Opinion of the German Association of Credit Institutes: *Stellungnahme der Deutschen Kreditwirtschaft e.V. zum Regierungsentwurf des Gesetzes zur Ergänzung des Geldwäschegesetzes*, sections 9a ff., GwG old version, German Federal Government Document (BT- Drs.) 17/10745 of 15 October 2012, 2.
[45] *Digital Rights Ireland* (n 33) para. 50.
[46] Case C-291/12 *Schwarz* [2013] ECLI:EU:C:2013:670, para. 42; similarly stated before by BVerfGE 125, 260, at 317.
[47] cf Baden-Württemberg State Parliament Document (LT-Drs.) 15/1707, 11-12.
[48] ibid. P Katko, 'Unlawful Internet Gambling Enforcement Act – Das Aus für das Internetglücksspiel in den USA?' [2007] Multimedia und Recht (MMR) 278, 281; L Oldag, in J Dietlein, M Hecker and M Ruttig (eds), *Glücksspielrecht* (2nd edn, CH Beck 2013) s 9 GlüStV para. 35.
[49] F Heseler, *Der Einfluss des Europarechts auf die mitgliedsstaatliche Glücksspielregulierung* (Nomos 2013) at 52.
[50] See Bolay and Pfütze (n 42) 122.

imposed on all parties involved alike: from the credit card issuers of the player to the acquiring bank of the operators of unlawful games up to the intermediary processor companies.[51] But not all parties have the same contractual proximity to the gambling operator and therefore are not all the same able to reliably identify unlawful games of chance.[52] Most likely, Financial Blocking will affect the issuing banks of the players, who – unlike the operators of unlawful games of chance – usually hold their bank accounts at domestic institutions. However, it is much more difficult to identify transactions connected with unlawful games of chance on the players' regular bank accounts than to identify payments received by the gambling operator for unlawful games of chance. Nevertheless, section 9(1) no. 4 of the GlüStV subjects all payments to Financial Blocking.[53]

cc. Lack of Proportionality

Finally, Financial Blocking measures lack proportionality as they lead to the proactive monitoring of all non-cash payment transactions of a total annual volume of around € 55 trillion and approximately 21 billion transactions per year.[54] This indiscriminate monitoring of all non-cash payment processes affects persons irrespective of any connection with unlawful gambling and is thus comparable to the general data retention by the providers of electronic communication services. Financial blocking, too, is to take place on a massive scale affecting a substantial part of the population and goes far beyond the objectives pursued. All available customer data, including that of persons not involved in unlawful games of chance, are used for permanent alignment without the data subjects' knowledge. Such permanent alignment without the knowledge of the persons affected is a particularly serious limitation of the data subjects' fundamental rights and freedoms. Article 8 of the EU Charter only permits preventative surveillance measures like the targeted retention of personal data for specific purposes. In order for the processing of personal data to be limited to what is strictly necessary, legislation must ensure that the scope of the measure is limited to certain

[51] See, to that effect, Bolay and Pfütze (n 42) 43; Brugger (n 6) 215.
[52] See, on this point, the criticism of the German Association of Credit Institutes: *Stellungnahme zur BaFin-Konsultation 02/2015 zu Mindestanforderungen an die Sicherheit von IT-Dienstleistungen*, 19 March 2015; for a detailed analysis on the criminal liability of the banks involved, see Rock and Seifert (n 32) 386.
[53] This is also criticised by Rock and Seifert (n 32) 383; in contrast, under 31 U.S.C. Sec. 5363 Unlawful Internet Gambling Enforcement Act ('UIEGA') the trader's bank is held primarily accountable: see Rock and Kaiser (n 32) 65–66; Katko (n 48) 280.
[54] Bundesverband deutscher Banken e.V. (ed), 'Zahlen, Daten, Fakten der Kreditwirtschaft' (Bankenverband, Berlin 16 November 2017) <https://bankenverband.de/media/publikationen/16112017_Zahlen_und_Fakten_web.pdf> accessed 27 March 2018.

categories of data and that it does not affect the population as a whole.[55] The more individuals are affected, the more severe such interference is as the permanent alignment of personal data can have an intimidating effect. Even the purpose of fighting serious crime, such as terrorism or organised crime, does not justify such a mass interference.[56] This must be even more true for the prevention of unlawful games of chance in the regulatory field of public security.

Aside from this, one must also take into account the freedom to exercise a profession or trade of the private entities involved. For instance, the freedom to conduct a business is curtailed when a provider is obliged, for the purpose of identifying suspicious transactions, to install "a complicated, costly, permanent computer system at its own expense"[57] – especially when considering the obligations already in place.[58] Payment services providers do not commonly collect the data required for blocking as part of their usual business activities but are made to collect and monitor data unrelated to their business.[59] A private player in the economy cannot be reasonably expected to monitor his services with "no limitation in time" and for "all future infringements" of legislative provisions by his customers.[60] The CJEU already held with regard to hosting providers and communication services that a measure requiring hosting service providers to install a filtering system to actively monitor almost all the data relating to its service users in order to prevent any future infringement of IP-rights was disproportionate.[61]

There is also a high risk of blocking lawful transactions in the context of games of chance (over-blocking).[62] Section 4(4)–(5) GlüStV no longer contains a general and consistent ban on online games of chance: as outlined above, online sports betting for example may be permitted under certain circumstances. This inconsistent approach makes it even more difficult for payment services providers to identify unauthorised operators among licensed operators with absolute certainty. If there is the risk that a monitoring system "might not distinguish adequately between unlawful content and lawful content, with the result that its

[55] *Tele2 Sverige* (n 17) para. 108; previously stated by BVerfGE 120, 378, para. 94; *PNR UE-Canada* (n 25) para 180.
[56] *Digital Rights Ireland* (n 33) para. 51; *Tele2 Sverige* (n 17) para. 102.
[57] The costs for businesses to comply with the recently tightened requirements of the Money Loundering Act (GwG) will amount up to 10.4 million €, see German Parliament Document (BT-Drs.) 18/11555, 92.
[58] See case C-360/10 *SABAM* [2012] ECLI:EU:C:2012:85, para. 46 concerning duties of hosting providers.
[59] See case C-212/11 *Jyske Bank Gibraltar* [2013] ECLI:EU:C:2013:270, para. 80.
[60] See case *SABAM* (n 58) para. 45 for compliance requirements of hosting providers in order to prevent the infringement of copyrights.
[61] ibid para. 37.
[62] These concerns have been addressed by authorities before, see Baden-Württemberg State Parliament Document (LT-Drs.) 15/1707, 12; Rock and Kaiser (n 32) 78; Koenig (n 7) 6.

introduction could lead to the blocking of lawful communications",[63] the rights of the persons concerned are unduly affected.

Furthermore, the Financial Blocking measure as provided for in the GlüStV is disproportionate because it does not contain exemptions from liability. Banks thus carry the risk of possible damage claims by customers for over-blocking as well as the investment and the contingency costs. In sum, all parties involved in the payment process will incur considerable extra costs that remain uncovered.

5. Performance of a Task in the Public Interest

As already shown, section 4(1) in conjunction with section 9(1) no. 4 GlüStV does not constitute a sufficient legal basis as required according to Article 6(3) of the GDPR. Therefore, the data processing measures required for Financial Blocking measures cannot be based on Article 6(1)(e) of the GDPR as well. This provision alone does not qualify as a legal basis, but only applies in conjunction with a special authorisation in the Member State legislation that meets the requirements of Article 6(3) of the GDPR. However, as already shown above, this is not the case.

6. Not Required to Pursue Legitimate Interests

Finally, data processing for Financial Blocking cannot be based on Article 6(1)(f) of the GDPR, allowing processing if this is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. The personal data is collected to combat unlawful games of chance and hence is pursued in the interest of the supervisory authority as a "third party" (see the definition in Article 4(10) of the GDPR). As in the case of the transfer of Passenger Name Record data by air carriers to US authorities, Financial Blocking also does not concern "data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security and for law-enforcement purposes".[64] But even if there might be a legitimate interest on the side of the supervisory authorities, processing will, according to Article 6(1)(f) of the GDPR not be considered lawful "where such interests are overridden by the interests or fundamental rights and freedoms of the data subject" concerned.[65] Considering that, as mentioned above, the far-reaching interference in the fundamental rights of the individuals enshrined in Article 7, 8 of the EU Charter is

[63] *SABAM* (n 58) para. 50 on content downloaded legally by users of social networks.
[64] Case C-317/04 *Parliament vs. Council* [2006] ECLI:EU:C:2006:346, para. 57.
[65] See also Case C-131/12 *Google Spain and Google* [2014] ECLI:EU:C:2014:317, para. 74.

particularly serious as well as the greats risks of Financial Blocking measures, the interests of the data subjects clearly outweigh public authorities' interests.

V. USING EXISTING DATA FOR ANOTHER PURPOSE

Financial Blocking not only requires the collection of new personal data by the banks involved. It will also require banks to use existing personal data for another purpose, i.e. combating unlawful games of chance, processing is incompatible with the GDPR. This is contrary to the strict purpose limitation as laid down in Article 5(1)(b) of the GDPR.

1. Purpose Limitation of Collected Data

The idea behind Financial Blocking is to make use of the huge amount of data that banks and financial institutions already dispose of, in order to assist the gambling supervisory authorities. For instance, banks collect various personal data of their clients when opening bank accounts or in order to comply with the "know your customer"-requirements under anti-money laundering legislation. For these purposes, they already report suspicious transactions to the competent authorities and retain certain categories of personal data of the parties involved in payment processes.[66] When opening an account, banks are obliged to collect personal data such as the name, place and date of birth, nationality, and address (section 9(1) no. 1, section 10(4) no. 1 GWG). In the case of money transfer additional data, such as the address, the ID-card number and the bank account numbers of the payer's payment account and of the beneficiary's account are processed.[67] Credit card institutes are obliged under section 25h(2), first sentence of the German Law on Credit ('KWG') to install data processing systems in order to screen individual transactions for money laundering, terrorist financing, and other criminal acts.

The further processing of this already existing personal data is subject to the strict purpose limitation of Article 5(1)(b) of the GDPR. The law only allows processing for the purposes of combating money laundering and terrorist financing (section 58 of the GWG; Article 15(2) of the Money Transfer Regulation) and "other criminal offences" that pose a risk to banks (section 25h(2) of the KWG and section 59(1) of the Payment Service Surveillance Act 'ZAG'). Combating unlawful games of chance, however, is not included in these limited

[66] cf Spoerr (n 19) 137; see J Milaj and C Kaiser, 'Retention of data in the new Anti-money Laundering Directive – 'need to know' versus 'nice to know'' (2017) 7(2) International Data Privacy Law 115.

[67] Art 4(1) and (2) Regulation (EU) 2015/847 of the European Parliament and the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (Money Transfer Regulation), OJ 2015 L 141, p. 1.

purposes. Also, organising and aiding in unlawful games of chance is no "other criminal offence" in the sense of section 25h(2) of the KWG.[68] This only includes such criminal offences at the expense of credit card institutions that might constitute a potential threat to the institution's assets and thereby lead to "an operational risk for a single institution, including legal or reputational risks".[69] Under German Criminal Law, only certain transactions made by operators of games of chance and not payments made by the players are relevant in terms of anti-money laundering regulations.[70] Simply assuming that participating in unlawful games of chance (that are prohibited for other reasons) per se constitutes an act of money laundering, or even financing terrorism, is much too general and vague and therefore not covered by the specified limited purpose of the cited regulations.

2. No Legal Basis for Processing Personal Data for the Purpose of the GlüStV

As the personal data was initially collected for the purpose of combating money laundering and terrorism financing, combating unlawful games of chance is no longer related to the initial purpose. Further processing of existing data for the purpose of Financial Blocking measures thus either has to meet the compatibility requirements stated in Article 6(4) of the GDPR or be justified by another legal basis. When assessing the compatibility of further processing operations with the purpose originally specified, the criteria as set out in Article 6(4)(a)–(e) of the GDPR shall be taken into account. This includes inter alia the question whether there is any link between the original purpose and the purpose of the intended further processing (a) or the possible consequences of the intended further processing for data subjects (d). In order to assess compatibility, the context in which the personal data have been collected and in particular, "the reasonable expectations of data subjects based on their relationship with the controller as to the further use"[71] must be taken into account. The interference entailed by Financial Blocking orders is, as stated above, far-reaching and likely to cause over-blocking, which potentially affects innocent customers, not involved in games of chance. Bank customers could not reasonably expect that their bank data will be further processed for the purposes of assisting gambling supervisory authorities in their combat of unlawful gambling. Therefore, using existing data for the purpose of Financial Blocking is not permitted by the original specified purpose.

[68] On the definition of the term 'other criminal acts' see Quedenfeld and Mühlroth in R Quedenfeld (ed), *Handbuch Bekämpfung der Geldwäsche und Wirtschaftskriminalität* (3rd edn, Erich Schmidt Verlag 2013) paras. 408–436.
[69] Explanatory memorandum of the German Federal Government (BT-Drs.) 17/3023, 60.
[70] Berberich and Kudlich (n 32) 184.
[71] Recital 50, sixth sentence of the GDPR.

Consequently, there needs to be a separate legal basis to further process the data. According to Article 6(4), first sentence of the GDPR, data may only be processed for another purpose without the data subject's consent if such further processing for another purpose is based on a law that constitutes a necessary and proportionate measure to safeguard the objectives stated in Article 23(1) of the GDPR. The general prohibition of participating in payments related to unlawful games of chance in section 4(1) of the GlüStV is a law with the objective of safeguarding the general public interests of a Member State within the meaning of Article 23(1)(e) of the GDPR. However, even if read in conjunction with section 9(1) no. 4 GlüStV, it lacks clarity and does not qualify as a precise legal basis under data protection law.

Financial blocking may lastly be justified under section 24(1) no. 1 of the BDSG. This provision allows data processing if it is "necessary" to safeguard public order or for the prevention of crime. Such restrictions under Member State law are allowed due the opening clause of Article 23(1) of the GDPR.[72] However, considering the severity of the interference with fundamental rights and freedoms, further processing is not "necessary". As an exception to certain principles laid down in Article 5 of the GDPR, the restrictions in section 24(1) of the BDSG must be interpreted in a narrow fashion.[73] The provision is not a blanket statement of authorisation for the permanent alignment of bank data without any cause for suspicion. It only authorises the transfer of data in individual cases and in case of actual suspicion. In the field of the prevention of threats to the public order, data transmission requires evidence for a specific and concrete danger.[74]

VI. OUTLOOK

The measure of Financial Blocking as provided for in the German gambling regulatory framework under the GlüStV in order to combat unlawful games of chance is incompatible with data protection law. Aside from this finding, the risks arising from the state's access to mass data stored by private entities are once again proven by the legislator's willingness to adopt measures of mass surveillance of financial transactions in order to prevent unlawful games of chance.[75] This tendency is not limited to Germany alone. Similar measures of

[72] German Federal Parliament Document (BT-Drs.) 18/11325, 96.

[73] See the case-law on art 15(1) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L 201, p. 37: *Tele2 Sverige* (n 17) para. 89.

[74] See P Kramer, in M Eßer, P Kramer and K von Lewinski (eds), *DSGVO/BDSG* (H Auernhammer (founder), 5th edn, Carl Heymanns Verlag 2017) s 28 BDSG para. 86.

[75] See M Rossi, 'Schutz der Privatsphäre – Aktuelle Gefährdungen' in H-J Papier, U Münch and G Kellermann (eds)*, Freiheit und Sicherheit* (Nomos 2016) 125ff.

Financial Blocking exist in many EU-Member States, while others plan to introduce them.[76] Austria for example considers introducing Financial Blocking in order to enforce their restrictive monopoly system, although credit institutions are already held liable under criminal law if they intentionally transfer assets to illegal gambling companies.[77] The GDPR aims at ensuring a high level of protection of individuals, which should be equivalent in all Member States. The problems highlighted above with view to the German Gambling Regulation are thus relevant for all national gambling legislation.

The EU Commission decided in December 2017 to close its infringement procedures and the complaints in the gambling sector in order to focus on its political priorities.[78] At the same time however, the EU Commission has given particular attention to the application of the data protection legislation in order to establish a digital single market but even more to ensure a high level of protection of personal data. Therefore, the violation of fundamental rights in order to defend national gambling monopolies should be of specific relevance to the EU Commission as well. The massive scale of Financial Blocking measures demonstrates the basic significance of the right to privacy not only as a freedom right, but over and above, as a precondition for the exercise of all fundamental rights and freedoms.

[76] For a country-by-country report see <http://www.europeancasinoassociation.org/country-by-country-report/> accessed 27 March 2018.
[77] See D Bereiter and S Storr, 'Gambling Policies and Law in Austria' in M Egerer, V Marionneau and J Nikkinen (eds), *Gambling policies in European Welfare States* (Springer 2018) 59–82.
[78] IP/17/5109 of 7 December 2017.