Taxpayers' Rights, the Right to Data Protection and Cybersecurity in the EU

Mylana Pfeiffer

Taxpayers' Rights, the Right to Data Protection and Cybersecurity in the EU

Mylana Pfeiffer[1]

[1] University of Luxemburg

Abstract. This paper mainly questions whether taxpayers can claim certain cybersecurity guarantees based on EU law. The author starts by introducing EU tax law, the notion of taxpayers' rights and why data protection and cybersecurity become more and more important in the field of EU tax law. Further, the author presents briefly what data protection and cybersecurity in a EU context mean and which impact it has on taxpayers. One main point of the study is to compare the data protection law and the cybersecurity law and the guarantees for taxpayers therein. Therefore, the paper outlines the intersections and divergences of EU data protection law and EU cybersecurity law. Another aspect of the paper is the question whether there is or even should be a taxpayers' right to cybersecurity.

Keywords: Taxpayers' rights, Cybersecurity, Data protection.

1 Introduction

All modern tax administrations use digital means in their daily tasks. Digital tools can consist of basic services, such as an online platform or an email address for communication or more advanced digital technologies, such as a virtual assistant for value added tax (VAT) or an automatic profit tax return. On the one hand, the use of these tools assures a good administrative practice and increases efficiency of the tax administrations. On the other hand, these constantly evolving technologies bring new challenges to assure taxpayers' rights. The legislators of all EU countries are fully aware of these difficulties and address them in various manners, among other things through law. For example, the German legislator introduced in May 2021 a new IT security act (IT-Sicherheitsgesetz 2.0) amending the "BSI" Act (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik). In France, the National Assembly's deputies fiercely discuss a new cybersecurity law in view of the increased risk. The EU reacted by issuing the Cybersecurity Act. Considering these legislative responses, it is time to ask whether taxpayers' rights keep pace with this development.

An important category of taxpayers' rights is the right to data protection. This right is of a strong public interest. Taxpayers share personal information with the tax administration trusting that their information will be held safe and confidential. This is only possible if high cybersecurity standards are assured. Does this mean, that taxpayers can

legally claim cybersecurity protection from the tax administration in relation to their personal data? This is not clear. Cybersecurity and data protection go hand in hand and cybersecurity is a precondition to a successful data protection. However, the fact that cybersecurity and data protection are related notions, does not guarantee their enforcement to be equal. The legal differences can be found in the meaning and scope of the legal bases to data protection and cybersecurity law, as well as in the obligations they impose on the tax administrations if they apply to tax administrations at all. This paper is only limited to the analysis of the EU Data Protection Regulation and parts of the EU Cybersecurity law. For the sake of brevity and coherence, the EU cybersecurity certification framework and other European legislation that might cover some aspects of cybersecurity, such as the EU Machinery Directive are not discussed herein.

Cybersecurity and data protection issues can arise in multiple scenarios creating different implications on taxpayers' rights. In this research, the author addresses the cybersecurity threats coming from outside, such as cyberattacks, putting at risk the protection of taxpayers' data. The internal threats, coming from whistle-blowers or the practice of naming and shaming are not dealt with in this study.

In Chapter 1 the author introduces the reader to EU tax law and the notion of taxpayers' rights. In Chapter 2 the author delineates the content and the limits of the taxpayers' right to data protection. Chapter 3 presents how the data protection law and the cybersecurity law interact with each other and which impact this interaction has on taxpayers' rights.

2 EU Tax Law, poor soil for taxpayers' rights?

Tax law is often perceived as a traditionally national matter in the hands of the States. To some extent it is still true. There is no tax administration at the EU level, nor is there a tax law code. It is up to the national tax administrations to ensure the collection of taxes. However, this important subject is not entirely outside the scope of EU law. One main priority of the EU Member States and the EU itself is to realize an effective Internal Market, including tax law. As a result, tax law has been progressively incorporated into EU law, which resulted in a patchwork. In metaphoric terms, the EU tax law patchwork consists of a harmonized VAT patch, a non-harmonized direct taxation patch, and an EU operated customs duties patch. The reason behind this step-by-step regulation is the EU's limited competence delineated in its founding treaties and the EU's undisputable talent to make something big out of very little. Similar to the ancient patchwork quilts that our ancestors sewed out of the little fabric in their possession, the EU tax law was progressively formed out of the legal spheres that the Member States were willing to manage at the EU level.

The non-homogeneous EU tax law leads to multiple complexities regarding the application of EU taxpayers' rights to EU taxpayers. The question of whether EU law

applies or not is a very important one and is always carefully analysed by the Court. But before reflecting upon this matter, what are taxpayers' rights?

The notion of taxpayers' rights is at once self-explanatory and extremely complex to define. It is self-explanatory because everyone has an idea of what it means or at least thinks to have an idea. It is complex because this idea does not provide for a general definition. In fact, there is no generally agreed definition of taxpayers' rights. For this reason, a literal interpretation seems to be a good start to interpret this notion. The English term "taxpayers' rights" and the French version of it "droits des contribuables" focus on the legal claims of persons who actually pay taxes. In German, there are two terms to describe a taxpayer, "Steuerzahler" and "Steuerschuldner". The latter is broader and englobes all persons who own taxes to the tax administration [1]. This understanding of the taxpayer notion focuses not on the moment of an actual payment of taxes, but on the moment when the claim to tax arises. In this case, even if an individual does not pay taxes, but should have paid them or will have to pay them, he is considered as a taxpayer. This broader personal scope of the term taxpayer seems to be the most suitable to interpret the notion of taxpayers' rights. Brzezinski also suggests such a broad definition and describes taxpayers' rights as rights "that belong to a taxpayer or other person in whom tax law is interested" [2]. This definition of taxpayers' rights would expand its scope to all persons finding themselves in a situation related to tax law. Also, this definition does not distinguish between fundamental rights and simple rights. One could suggest that the notion of taxpayers' rights englobes all rights, fundamental and regular ones. However, many publications on taxpayers' rights refer to taxpayers' fundamental rights or fundamental principles when talking about taxpayers' rights [3] [4] [5]. These are sometimes referred to as basic rights in hands of taxpayers or the minimum standard of protection of taxpayers [6]. This is especially true for discussions on the bill or the Charter of taxpayers' rights refer to fundamental rights [7]. Fundamental rights are certainly the most essential rights that need to be defended, especially if one seeks to achieve the minimum standard of protection at an international level. Here it is important to note that fundamental rights are most of the time implemented through regular rights, which contribute to their effectiveness. Therefore, it is important to consider all layers of law when studying taxpayers' fundamental rights.

As to the Court, it generally ignores this notion in its case law and refers to "the right for the taxpayer" [8] or "taxpayer has certain rights under the Charter" [9].[1] This can be explained by the fact that this notion does not appear in any primary or secondary law of the EU. This notion being absent from EU law and case law, it is not possible to define it with certainty.

[1] The Court mentions "taxpayer's right" once in the Sabou case, but not in the meaning of a general taxpayer's right, rather as an abbreviation for the right to the taxpayer.

However, several EU non-legislative and non-binding documents address taxpayers' rights. For instance, the Package for fair and simple taxation [10] including the Action Plan for fair and simple taxation in 2020 [11]. In addition, since at least a decade the Commission elaborates on a Taxpayer Charter at the EU level [12] [13]. In the end, it decided to publish the Taxpayer Charter in form of a Roadmap which aims at listing taxpayers' existing rights [14] [15]. It is called Communication on Taxpayers' Rights in the Single Market and is meant to englobe the whole relevant case law on this matter. It will apply to the direct and the indirect taxation and will probably list some fundamental rights as well as secondary rights [16]. At this moment, the document still needs to be adopted by the Commission but is announced to be published in the third quarter of 2021. Furthermore, the European Taxpayers' Code has been published in 2016 and specifies on its front page that it is a non-binding instrument meant to provide for a guideline and best practices of taxation, but only of a purely informative character [13]. Its major aim is to contribute to easier tax compliance and therefore prevent tax fraud, evasion and avoidance. It contains a list with 9 general principles, such as data protection, privacy and respect of law [13]. The guidelines specify that the principles listed are not part of EU law but a compilation of principles that can be found in all Member States [13].

And again, none of these documents of the European Commission define the notion of taxpayers' rights. They provide a list of shared principles across the Member States and/or present rights that the taxpayers already have under EU law [17]. At least, the reference to taxpayers' rights in the political documents of the European Commission confirms that this notion exists at the EU level.

To conclude, the current EU tax law is certainly not the richest ground to yield strong taxpayers' rights and it is up to the Member States to assure that taxpayers' rights are guaranteed. The aforementioned non-binding instruments of the Commission will improve the awareness of the existing taxpayers' rights but will not expand or add new taxpayers' rights at the EU level. The legal problems of situations where taxpayers find themselves in a legal gap without protection will continue to subsist even after the publishing of the Communication [18].

3 The taxpayers' right to data protection

3.1 EU data protection

The early traces of the EU data protection law can be already found in a Communication of the Commission in 1973 [19]. Primary law refers to data protection in Art. 8 of the Charter and Art. 16 Treaty on the Functioning of the European Union (TFEU). The first piece of secondary legislation only appeared in 1995 in the form of the Directive 95/46/EC, which is now replaced by the General Data Protection Regulation (GDPR).

In addition, the Directive 97/66/EC [20] aimed to fortify data protection specifically in the telecommunications sector and was revised with the Directive 2002/58/EC [21].

The two different layers of data protection at the EU level, primary and secondary, must be distinguished. Primary law is formed by the founding treaties, the Charter of fundamental rights and the general principles of the EU. It applies directly to the Member States and the EU organs [22]. Secondary law is made by the EU organs and implements primary law. The primary law rules over secondary law.

Art. 16 (1) TFEU simply states that everyone has the right to the protection of personal data without going into detail. Art. 16 (2) TFEU confers competence to the EU to foresee the details of this right into secondary legislation [23]. In the EU case law on the right to data protection, the Court does not use this legal basis but directly refers to the secondary legislation and the Charter. Before the Charter became binding, the Court referred to the general principles defending the fundamental rights. The Charter [24] is a constituent of primary law and has the same legal value as the Treaties (Art. 6 (1) TEU). In its Art. 8, the Charter grants protection of personal data. It reads:

"Article 8 - Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

Different elements of this provision need to be further commented.

First, the protection of this article is activated when personal data is processed. This is an important element, because in contrast to the right to private and family life protected in Art. 7 of the Charter, there is no need to prove an interference with privacy for this right to apply [25]. In Art. 8 of the Charter, there is no need to prove an interference and the simple fact of data processing offers the protection. The protection consists of a guideline setting minimum guarantees about how to lawfully process the data.

Second, the right to the protection of personal data is constituted by 5 underlying guarantees: The fair processing, the processing for specified purposes, the legitimate basis by law or by consent, the access to data, the right to rectification of data and an independent supervision. The Charter did not invent the fundamental right to data protection. It reaffirms what has already existed, be it in secondary law, the Convention 108 and a number of political documents. Therefore, the content of Art. 8 of the Charter can be explained with the help of the GDPR, the most important secondary legislation in the data protection field [26]. The GDPR implements the fundamental right of data protection anchored in the Charter and makes this right effective [27]. It also defines rather broad concepts. From the Recital 39 of the GDPR we can read that the concept of fairness is connected to the transparency principle. The principle of transparency in

this context requires that the information shared with the individual on the processing of his personal data should be "easily accessible and easy to understand, and that clear and plain language be used".[2] The expression processing for specified purposes refers to the purpose limitation principle. It means that data collected for a specified purpose cannot be processed repeatedly for other purposes than the initial one. The legitimate basis by law or by consent requires for a legal or consensual basis prior to the data processing. The right to access information can be activated by the data subject on request and is relevant for the use of the right to rectification of personal information. The independent supervision is an independent public authority in every Member State that monitors the efficiency of data protection law. Finally, it needs to be noted that there is no mention or reference to cybersecurity. The fundamental right to data protection only focuses on the rights of a person concerning its data, ignoring the threats coming from outside and the obligations of the processor or controller to keep the data safe.[3] Therefore, it can be claimed that there is no fundamental right to data protection in the sense of a securitization of data. There is only a fundamental right to data protection in form of a code of conduct of how process personal data guaranteeing the minimum rights of a person when its data is processed.

Comparing the Charter to the GDPR, the GDPR has a much richer catalogue of rights and obligations. Of course, the Charter contains only one article of 3 paragraphs on data protection in contrast to the GDPR which consists out of 99 articles on 88 pages. Also, the Charter and the GDPR pursue different aims [27]. While the Charter is a fundamental right that protects a minimum the personal data of each one to whom EU law applies, the GDPR has a broader aim to ensure that this right is effectively protection in harmony with other fundamental rights and fundamental freedoms [27]. Thus, the act of comparison can only result in differences. The differences can also be found in the application of the different legal bases of data protection law to taxpayers.

3.2 The application of the data protection right to taxpayers

The first question to ask before applying EU law is whether EU law governs a situation. Purely national scenarios or situations outside the scope of EU law are not regulated by EU law. There must be a linking event in a case connecting it to EU law. Art. 51 (1) of the Charter delineates its scope to situations that implement EU law. Also Art. 6 (1) TEU announces that the Charter shall not extend EU competences. The GDPR states explicitly in its Art. 2 (2) (a) that it does not apply "in the course of an activity which falls outside the scope of Union law".

This is a very serious criteria, especially when it comes to the application of fundamental rights. This question has been dealt by the Court decades before the existence

[2] Recital 39 GDPR.

[3] This statement does not refer to the GDPR, which is secondary law. It only discusses the content of the fundamental right to data protection included in the Charter.

of the Charter. Before the Charter, the fundamental rights were protected by the Court through general principles of EU law [28]. The most prominent cases prior to the Charter concerning the application of fundamental rights are the *ERT* case, the *Wachauf* case and the *Annibaldi* case. These three cases show the three possible situations of application and non-application of EU general principles of fundamental rights. The *ERT* case refers to a national law that constitutes an infringement to the freedom to provide service. The Court held that the justification to this infringement needed to be "interpreted in the light of the general principles of law and in particular of fundamental rights" [28]. The *Wachauf* case [29] concerns the application of fundamental rights to situations where national authorities implement EU secondary law, in this case a Regulation. The *Annibaldi* case gives an example of a situation where EU law does not apply and therefore the Court did not assess the fundamental rights [30]. The case law since the coming into force of the Charter in the field of taxation interprets more specifically what Art. 51 (1) of the Charter means by "implementing Union law". In 2013, the Court stated in the *Akerberg Fransson* case, with a reference to the *ERT* case, that "the fundamental rights guaranteed in the legal order of the European Union are applicable in all situations governed by European Union law, but not outside such situations" [31]. It explained further that such situations are when Member States "act in the scope of Union law" [31]. This case covers an active behaviour of a Member State. This is due to the specific facts of the case, where Mr. Fransson was accused of providing false information in his tax returns of income and VAT. He was pursued in administrative and criminal instances and claimed the ne bis in idem principle to apply protected by Art. 50 of the Charter and Art. 4 of the Protocol No. 7 to the ECHR. The Court revealed a link between Mr. Fransson's VAT offences and the EU budget which must be protected according to Art. 325 TFEU. Also, it specified that as VAT is regulated at the EU level, the illegal activities of Mr. Fransson enter the scope of EU law. The Member State's active behaviour of penalizing such activities falls into the scope of the EU law, even if the VAT directive does not foresee penalization [31]. This argument was confirmed in the *Berlioz* case [8]. A couple of months later in 2013, the Court judged in the *Sabou* case that the Charter is applicable to cases where Member States apply EU law, in this particular case the mutual assistance procedure Directive 77/799, even if the EU law did not oblige the Member States to do so in the scenario of the case. The decision of a Member State to apply EU law is sufficient to open up the scope of application of the Charter [9]. The very recent *D. H. T* case demonstrates that the Charter does not apply to situations where national law expands the scope of a EU Regulation and applies the GDPR provisions also to legal persons, and not only to natural persons as initially foreseen by the GDPR [32]. Germany expanded the scope of the GDPR in order to grant the same data protection to natural and legal persons. In this case and in contrast to the *Akerberg Fransson* case, the national measures were not necessary for the implementation of the GDPR. Therefore, the situation had no connecting element to EU law to make the Charter applicable. In the *Belgische Staat* case, the Court judged the case as

inadmissible regardless the fact that the facts were linked to VAT fraud. This is because the case grounded on the use of evidence from criminal proceedings linked to VAT fraud to reassess the income tax, which is not regulated by EU law and therefore falls out of its scope. The analysis of the recent tax case law in relation to the application of the Charter shows that there must be a connecting element linking a situation to EU law. In other words, if the situation is somehow ruled by EU law the Charter applies. This link does not have to be immediately perceptible like in the *Akerberg Fransson* case.

Regarding the material scope of application, neither the TFEU, nor the Charter exclude the application of data protection law to an EU tax law context. These are general provisions applying to all fields of EU law. The GDPR does not exclude tax administrations out of its scope, neither. The Court confirmed the application of the GDPR to tax administrations in the *Puskar* case. The questions of the case referred to the interpretation of the data protection directive but are also valid for the GDPR that replaced the directive. The Court stated that "the collection (of data) and their use by the various tax authorities at issue in the case in the main proceedings therefore constitute 'processing of personal data' within the meaning of Article 2(b) of that directive". It further reads that the objective of the tax administrations to collect and process information are linked to the objective of a controller. Therefore, the tax administrations have to respect the obligations in the GDPR.

As to the personal scope, Art. 16 (1) TFEU grants the data protection to everyone. The wording of the Charter as well does not distinguish between natural or legal persons. It could be argued that the way the Art. 8 of the Charter is formulated "everyone has protection… concerning him or her" indicates that it applies only to natural persons. The Court interpreted that Art. 8 of the Charter does not grant the same level of protection to legal persons as it does to natural persons [32]. By ruling this the Court refers to the ECHR case law in relation to Art. 8 ECHR. However, it does not say that there is no protection at all, and the ECHR has shown that legal persons also have rights protected by Art. 8 of the ECHR. The GDPR, however, explicitly limits its scope to natural persons.

If the Charter opens new opportunities for taxpayers, they are not unlimited, and the restricted scope of application has always to be considered [33]. Case law shows that the Charter covers all situations with a connection to EU law. It also shows that there are still situations falling entirely out of scope where taxpayers are only covered by national or international law. But even for situations falling into the scope of the EU data protection law, the right to data protection is not absolute. The data protection rights in the Charter as well as in the GDPR even if applicable can be restricted. Art. 52 of the Charter provides general conditions of restriction that apply to all fundamental rights of the Charter. For a restriction to be valid, it needs to have a legal basis. It further has to pass the proportionality test, testing the aptitude, the necessity, and the strict proportionality of the restrictive measure [34].

As to the GDPR, Art. 23 GDPR lists grounds of restrictions to some of the rights and obligations of the regulation in addition to its restricted scope.[4] Art. 23 (e) GDPR mentions "other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security".[5] This restriction serves in the interest of Member States and against the taxpayer's interests, but should not decrease taxpayers' rights excessively as Art. 23 (1) GDPR states that they must have a legal basis and respect "the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society".

To conclude, the taxpayers' fundamental right to data protection defends the taxpayers' data against unlawful processing and offers the taxpayers guarantees comparable to minimum standards about how data should be processed. Its scope is limited but generally applies to taxpayers.

4 Cybersecurity for all, except for taxpayers?

4.1 The narrow scope of application of the EU Cybersecurity law

The NIS directive [35] is presented by the European Commission as "the first piece of EU-wide legislation on cybersecurity" [36]. This might be true in the sense that the NIS directive is a specific legislation on cybersecurity, but not in the sense that no other instrument addressed cybersecurity before. Some aspects of cybersecurity have already been addressed in other legislation, among others in the GDPR.[6] The NIS also has a rather narrow scope of application [37] and does not apply to tax authorities. It follows a different aim than the GDPR. While the NIS directive aims to secure the network and information security and the data therein, the GDPR targets the risks to personal data of individuals. This may devalue to some extend the NIS directive in the tax law context. It is still worth to present this directive as it explains what the current regulation on cybersecurity is.

Reading the NIS directive [35], the reader will disappointedly realise that the term of cybersecurity appears only once in its recital, and only when talking about "international cooperation on cybersecurity".[7] Instead, in its title and in all its articles it refers

[4] Art. 2 (2) of the GDPR.

[5] Further described in Rec. 112 GDPR. This restriction has also been cited in (Art. 3 1. b) of the Decision of the Management Board of the European Union Agency for Cybersecurity of 21 November 2019 on internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of ENISA PUB/2020/96 OJ L 37, 10.2.2020.

[6] The GDPR came into force approximately two months before the NIS directive.

[7] Recital 34 NIS directive.

to "security of network and information systems".[8] In contrast, the proposal for a revised NIS directive includes the notion of cybersecurity 140 times, including in the title [38]. The proposal to revise the directive aims at overcoming the deficiencies of the NIS directive, by inter alia expanding the scope of application to all large and medium companies and providing for a standard of security measures to tackle cybersecurity challenges. The proposal refers to the EU Cybersecurity Act Regulation [39] which includes a definition of cybersecurity. The EU Cybersecurity Act gives a permanent mandate to the EU Agency for cybersecurity to manage the ICT certification in the EU, to increase cooperation between the Member States and to support them in case of cybersecurity related problems. This regulation is interesting because it introduces new notions and definitions at the EU level. It defines in its Art 2 (1) cybersecurity as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats". It further reads that "'cyber threat' means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons".

With the constant digitalization and automation of the public sector, taxpayers' data also face cyber threats and only high standards of cybersecurity can guarantee their protection. But as already noted above, the NIS directive does not apply to tax administrations and taxpayers cannot claim cybersecurity rights based on this particular legislation. The larger scope of application of the proposal for a revised NIS directive includes public administrations, but only to a certain kind of public administrations.[9] It seems that there is no political will to include tax administrations into the scope of the revised directive.[10] First, because the Annex I to the proposal lists the administrations to whom the revised NIS directive would apply, and tax administrations are not mentioned in it. This list refers only to the public administration entities of central governments and some public administration entities of NUTS (territorial units for statistics) [40]. Second, a working document of the Commission states that the aim of the revised directive is to include public administrations "in its function of provider of services to citizens and businesses that are essential for the functioning of the internal market" [41]. Tax administrations are generally not considered to be service providers. Their main aim is to collect taxes for the State. This may contribute for the well-functioning of the internal market, for example by guaranteeing financial stability in the EU, but is not essential in the sense of an economic driver. Lastly, even if tax

[8] See the title of the NIS directive.

[9] Art. 2 (1), (2) and Art. 4 (23) Regulation (EU) 2019/881. This can also be read from the detailed explanation of the proposal p. 9: Annex I (energy; transport; banking; financial market infrastructures; health, drinking water; waste water; digital infrastructure; public administration and space).

[10] Art. 4 (23) Regulation (EU) 2019/881. "Public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security are excluded".

administrations would be considered as public administrations that provide services, they would fall under the exception of law enforcement foreseen in Art. 4 (23). Therefore, there is no cybersecurity right based on the NIS directive that would apply in a tax law field and eventually grant taxpayers a right to cybersecurity. This can be explained by the fact, that the EU is still mainly driven by economic considerations. It is a priority of the EU to regulate the life of economically relevant subjects, such as companies or entrepreneurs. One could argue that a general cybersecurity legislation applicable to all actors, including tax administrations would be beneficial for cross-border workers and companies. It would provide legal certainty and trust in all Member States and contribute to the freedom of movement of workers and the freedom of establishment. But the harmonization has not still achieved this level. The public opinion is still divided on the question of whether the NIS Directive should or should not include further public sectors into its scope of application [41]. While cyber professionals approve such a wide-reaching cybersecurity directive, OESs, DSPs and trade associations are against it ("Cyber professionals were more likely to agree to extend the scope of the NIS Directive to include further sectors and types of digital service at risk of cyber threats. On the other hand, OESs, DSPs and trade associations were far less likely to agree with 22.8% and 25% of them respectively disagreeing with the prospect of including further digital services within the scope of the NIS Directive") [41]. It is therefore very unlikely that a taxpayers' right to cybersecurity will see the light under cybersecurity legislation.

This does not mean that taxpayers are denied cybersecurity. All States across the world are aware of the risks and costs of an insufficient cybersecurity protection. Regrettably, it is difficult to say with certainty how much the Member States spend on cybersecurity and the investment in strong cybersecurity can only be guessed relying on different factors [42]. To reassure the taxpayers, the cybersecurity guidelines of the NIS directive through the application to businesses are believed to create a certain level of herd immunity in a cyberspace where everything is interlinked [43]. Finally, a taxpayers' right to cybersecurity could be deduced from the GDPR, or lastly from a national or an international law.

4.2 Can a taxpayers' right to cybersecurity be deducted from data protection law?

On the one hand, the link between cybersecurity and data protection is undeniable. For instance, the proposal for the NIS directive mentions the improved personal data protection for citizens as its indirect benefit [38]. A Commission's communication reads: "Cybersecurity is essential … for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data" [44]. In a digital world, there is no data protection without a strong cybersecurity regulation. On the other hand, the data protection law and the cybersecurity law have different legal bases. Despite their intersections, they do not cover the same situations and pursue different aims. One striking difference is that the fundamental right to data protection in Art. 8 of the Charter does not mention cybersecurity at all. The cybersecurity aspects of the

right to data protection are only addressed in the GDPR. There is therefore no taxpayers' fundamental right to cybersecurity in EU law but a legal claim to cybersecurity in certain situations granted to natural taxpayers based on the GDPR.

The GDPR provides for cybersecurity guidelines in Articles 25 and 32 of the GDPR. Art. 25 GDPR is the legal basis for the by design and by default principle. By design means that the data protection considerations need to be incorporated at the stage of designing the products [23]. According to Art. 25 GDPR controllers have to implement adequate technical solutions to guarantee the rights of the data subjects [45]. The protection by design and by default principle is considered to encourage "to take into account the right to data protection when developing and designing such products"[11] and therefore to have a preventive and proactive effect on the data protection of data subjects. The GDPR gives examples of data protection by design, such as "minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features".[12] More specifically, Art. 32 relates to the security of processing and forces the controllers and the processors to foresee technical measures such as "(a) the pseudonymisation and encryption of personal data (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing." These are technical provisions relating to cybersecurity. In both provisions, the obligation goes only as far as the state of the art permits it and "the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons" are balanced.

The state-of-the-art concept is intended to be broad and dynamic evolving through space and time, to keep pace with the technological developments in the IT security field. The understanding of this concept is based on practice. The Guideline "State of the art" published by the German IT Security Association TeleTrusT in cooperation with the European Network and Information Security Agency (Enisa) provides for an orientation for practitioners and other interested parties on the current understanding of the state of the art.[13] Taxpayers can also rely on the state-of-the-art concept to claim the protection of their data based on the GDPR. Art. 25 and Art. 32 of the GDPR oblige the controllers and/or processors to take "into account the state of the art" when elaborating the data protection by design and by default, and the security of processing.

---

[11] Recital (78) GDPR.
[12] Recital (78) GDPR, these examples are also in Art. 25 (1) GDPR.
[13] The Guideline dates from 2021, an update is foreseen every two years.

The tax administrations need to guarantee this level of cybersecurity protection at least to the taxpayers that are natural persons. Another interesting fact is that the restrictions to some rights and obligations of the Regulation foreseen in Art. 23 GDPR do not apply to cybersecurity guidelines. This can be explained by their specific nature that need to be technically implemented without exception.

Comparing the technical implementation of cybersecurity requirements between the NIS directive and the GDPR, one can conclude that even here the GDPR goes further than the NIS does. While Art. 14 and Art. 16 of the NIS Directive mention that cybersecurity must go as far as the state of the art permits it, they do not go further into details. They also impose obligations on the Member States. They have to ensure that "operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations" (Article 14(1) NIS) or "that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems" (Article 16(1) NIS). Compared to the GDPR, the NIS directive creates rather vague obligations and makes it clear that is up to the Member States to assure the security of the network and information systems. This is not surprising and can be explained by the fact that the NIS directive is a directive, which in its nature leaves the implementation of harmonized principles up to the Member States. The GDPR is a regulation, therefore directly applicable and transposable as such in the Member States. Considering the aforesaid, the fact that the NIS directive does not apply to tax administrations and grants no claim to taxpayers to cybersecurity, has no impact on taxpayers. Compared to the NIS directive, the GDPR seems to be more appropriate in its aim and scope of protection to defend taxpayers' rights regarding data protection and cybersecurity.

The GDPR is an instrument like no other and is sometimes referred to be the law of everything [46]. With its broad scope of application and its content in relation to data protection and cybersecurity, it guarantees taxpayers cybersecurity protection even if only within the limits of the GDPR. This does not create a new taxpayers' right to cybersecurity, but rather addresses cybersecurity as a technical aspect of the taxpayers' right to data protection. For example, a taxpayer can claim from the tax administrations to guarantee the pseudonymisation or encryption of personal data. But these cybersecurity measures operate only in the scope of the GDPR. This means that from a strict legal point of view there is no general legal obligation to adapt this cybersecurity measure, but only a specific one in the limits of the processing of personal data and only as far as the GDPR applies. Although it is desirable to have a general obligation to cybersecurity in all fields of data processing, this is still not the case. As the Working Party 29 declares in one of its statements, "the availability of strong and efficient encryption is a necessity in order to guarantee the protection of individuals with regard to the confidentiality and integrity of their data" [47]. Encryption being one of the cybersecurity obligations in the GDPR, it is presented as a means to a greater end.

5 Conclusion

The limited competence of the EU in the EU tax field makes the application of taxpayers' rights a complex matter. The application of EU law and the scope of application of the relevant legislation has always to be carefully tested before a taxpayer can have the certainty to claim rights. The right to data protection is guaranteed in the Charter, the TFEU and secondary legislation and generally applies to taxpayers. This is not the case for cybersecurity. The NIS directive, which harmonizes cybersecurity guidelines in the EU, does not pursue the aim to secure personal data and does not apply to tax administrations. Even if there is a link between data protection and cybersecurity, there are also striking differences in their legal meaning and application. While there is a fundamental right to data protection, there is no fundamental right to cybersecurity. The fundamental right to data protection of the Charter does not foresee any requirements relating to cybersecurity. As to the secondary law, taxpayers can claim the application of certain cybersecurity measures when the GDPR applies. The GDPR only ensures that tax administrations implement cybersecurity guidelines when acting as controllers or processors and when processing personal data. This is not a general right and is only applicable to situations falling under the scope of the GDPR. The author therefore reaches the conclusion that there is no stand-alone taxpayers' right to cybersecurity.

Looking back to the last century, there was no fundamental right to data protection. However, with the changing digital environment it cut itself off from the more general right to privacy. Cybersecurity becoming more and more important in our society, the question comes up whether it could become a stand-alone right over time? Some want cybersecurity to be recognized as a human right, [43] [48] some do not want that the scope of its application expands further [41]. And should cybersecurity become a general fundamental right applicable to all, what should it look like? As for now, cybersecurity is far from being a general right and even further from becoming a fundamental right of EU law.

References

1. Lexikon der Wirtschaft, https://www.bpb.de/nachschlagen/lexika/lexikon-der-wirtschaft/20760/steuerzahler, last accessed 2021/09/01.
2. Brzezinski, B.: Taxpayers' Rights: Some Theoretical Issues. In: Nykiel, W., Sek, M. (eds.) Protection of taxpayer's rights, European, International and Domestic Tax Law Perspective, pp. 17-32. Oficyna Wolters Kluwer Business, Warsaw (2009).
3. Confédération Fiscale Européenne,
   Model Taxpayer Charter, http://www.taxpayercharter.com/charter.asp?id=15, last accessed 2021/10/05.

4. Platform for Tax Good Governance, Corporate Tax Policy Key Priorities Q&As September 2020, https://ec.europa.eu/taxation_customs/sites/default/files/confederation_fiscale_europeenne_tax_advisers_europe.pdf, last accessed 2021/10/05.
5. Savvas, K.: European Union - EU Whistle-blower Directive: Taking Taxpayers' Rights Seriously. World Tax Journal 13/2, (2021).
6. Pistone, P., Baker, P.: The Practical Protection of Taxpayers' Rights. IFA cahiers de droit fiscal international 100b, (2015).
7. Bowal, P., Wanke, I.: Taxpayers' rights. Law Now 23(4), (1999).
8. Judgment of the Court (Grand Chamber) of 16 May 2017, Berlioz Investment Fund SA v Directeur de l'administration des contributions directes. Case C-682/15. ECLI:EU:C:2017:373.
9. Judgment of the Court (Grand Chamber) of 22 October 2013, Jiří Sabou v Finanční ředitelství pro hlavní město Prahu. Case C-276/12, ECLI:EU:C:2013:678.
10. European Commission Press Release,
15 July 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1334, last accessed 2021/09/01.
11. Brussels, 15.7.2020 COM(2020) 312 Final Communication from the Commission to the European Parliament and the Council, an action plan for fair and simple taxation supporting the recovery strategy.
12. Confédération Fiscale Européenne: Towards greater fairness in taxation, A Model Taxpayer Charter, Presentation to the members of the Platform for Tax Good Governance, (2014), https://ec.europa.eu/taxation_customs/sites/default/files/resources/documents/taxation/gen_info/good_governance_matters/platform/meeting_20140610/cfe.pdf, last accessed 2021/10/02.
13. EU Commission, Guidelines for a Model for a European Taxpayers' Code, Ref. Ares(2016)6598744 - 24/11/2016 https://ec.europa.eu/taxation_customs/sites/default/files/guidelines_for_a_model_for_a_european_taxpayers_code_en.pdf, last accessed 2021/09/01.
14. Brussels, 15.7.2020 COM(2020) 312 final Annex, annex to the Communication from the Commission to the European Parliament and the Council, an action plan for fair and simple taxation supporting the recovery strategy.
15. Brussels, taxud/d1(2021) summary record of the meeting of the platform for tax good governance held online on 10 March 2021.
16. Initiative for Taxpayers' Rights - Proposal for a Recommendation to improve the Situation of EU Citizens as Taxpayers for Direct and Indirect Tax, https://ec.europa.eu/taxation_customs/sites/default/files/210310_platform_meeting_-_taxpayers_rights_paper.pdf, last accessed 2021/09/01.
17. Questions and Answers on the Tax Package,
15 July 2020, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1337, last accessed 2021/09/01.
18. Chaouche F., Haslehner, W.: Cross-Border Exchange of Tax Information and Fundamental Rights. In: Haslehner, W., Kofler, G., Rust, A. (eds.) EU Tax Law and Policy in the 21st Century, EUCOTAX Series on European Taxation, vol. 55, pp. 179-212. Wolters Kluwer, Alphen aan den Rijn (2017).

19. González Fuster, G.: The Materialisation of Data Protection in International Instruments. In: The Emergence of Personal Data Protection as a Fundamental Right of the EU. Law, Governance and Technology Series, vol 16, pp. 75-107, Springer, Cham. (2014).
20. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.
21. 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) Official Journal L 201, 31/07/2002 pp. 37-47.
22. Schaumburg, H.: Einführende Grundlagen. In: Schaumburg, H., Englisch, J., Fehling, D., Kofler, G., Oellerich, I., Reimer, E. (eds.) Europäisches Steuerrecht, Otto Schmidt KG Verlag, Köln (2015).
23. Savin, A.: EU Internet Law. 2nd edn. Elgar European Law, Massachusetts (2017).
24. Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, pp. 391-407.
25. Docksey, C.: Articles 7 and 8 of the EU Charter: two distinct fundamental rights. In: Grosjean, A. (ed.) Enjeux européens et mondiaux de la protection des données personnelles, pp. 71-97. Larcier, Brussels (2015).
26. 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).
27. Ausloos, J.: Foundations of Data Protection Law. Oxford University Press, New York (2020).
28. Judgment of the Court of 18 June 1991, Elliniki Radiophonia Tiléorassi AE and Panellinia Omospondia Syllogon Prossopikou v Dimotiki Etairia Pliroforissis and Sotirios Kouvelas and Nicolaos Avdellas and others (ERT). Case C-260/89. ECLI:EU:C:1991:254.
29. Judgment of the Court (Third Chamber) of 13 July 1989, Hubert Wachauf v Bundesamt für Ernährung und Forstwirtschaft. Case 5/88. ECLI:EU:C:1989:321.
30. Judgment of the Court (First Chamber) of 18 December 1997, Daniele Annibal-di v Sindaco del Comune di Guidonia and Presidente Regione Lazio. Case C-309/96. ECLI:EU:C:1997:631.
31. Judgment of the Court (Grand Chamber) of 26 February 2013, Åklagaren v Hans Åkerberg Fransson. Case C 617/10. ECLI:EU:C:2013:105.
32. Judgment of the Court (First Chamber) of 10 December 2020, Land Nordrhein-Westfalen v D.-H. T. as liquidator of J & S Service UG. Case C-620/19, ECLI:EU:C:2020:1011.
33. Kokott, J.: European Union - Taxpayers' Rights. European Taxation 60(1), (2020).
34. Placco, A.: La protection des données à caractère personnel dans le cadre de la jurisprudence de la cour de justice de l'Union Européenne relative aux droits

fondamentaux. In: Grosjean, A. (ed.) Enjeux européens et mondiaux de la protection des données personnelles, pp. 31-50, Larcier, Bruxelles (2015).
35. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union OJ L 194, 19.7.2016, pp. 1–30.
36. NIS Directive, https://digital-strategy.ec.europa.eu/en/policies/nis-directive (17.06.2021).
37. Cole, M., Schmitz, S.: The Interplay between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape. University of Luxembourg Law Working Paper No. 2019-017, (2019).
38. Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 COM/2020/823 final.
39. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)(OJ L 151, 7.6.2019, p.15)
40. Regulation (EC) No 1059/2003 of the European Parliament and of the Council of 26 May 2003 on the establishment of a common classification of territorial units for statistics (NUTS) (OJ L 154, 21.6.2003, p. 1).
41. Brussels, 16.12.2020 SWD (2020) 345 final Part 2/3 Commission Staff Working Document Impact Assessment Report.
42. Antczak, J., Kamiński, K.: Cybersecurity Expenditure in the EU Member States for the non-profit organisation. New Direction, Brussels (2018).
43. Shackelford, S.: Should Cybersecurity be a Human Right: Exploring the Shared Responsibility of Cyber Peace. Stan J Int'l L 55(155), (2019).
44. Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade JOIN/2020/18 final.
45. Tamò-Larrieux, A.: Privacy and Data Protection Regulation in Europe. In: Designing for Privacy and its Legal Framework. Law, Governance and Technology Series, vol 40, Springer, Cham (2018).
46. Purtova, N.: The Law of Everything. Broad Concept of Personal Data and Overstretched Scope of EU Data Protection Law. Law, Innovation and Technology 10(1), 40-81 (2018).
47. Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU, Brussels, 11 April 2018.
48. Human Rights Watch, 26 May 2020 https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue, last accessed 2021/09/01.