WIRTSCHAFTSUNIVERSITÄT WIEN

Vienna University of Economics and Business

EU-GDPR:

AN EFFECTIVE PROTECTION OF CITIZENS' PERSONAL DATA?

EU-DSGVO: EIN WIRKSAMER SCHUTZ DER PERSÖNLICHKEITSRECHTE DER BÜRGER?

Date: 18th June 2018

Author, ID: Christoph Haberhauer, 01352204

Course: SBWL BIS K5 Wirtschaftsinformatik-Projektseminar 4219, SS18

Examiner: ao.Univ.-Prof. Mag. Dr. Rony G. Flatscher

Table of Contents

List of Abbreviations

Abs	Paragraph (Absatz)
AHG	Amtshaftungsgesetz
Art	Article
BGBl	Bundesgesetzblatt
BDSG	Bundesdatenschutzgesetz
B-VG	Bundes-Verfassungsgesetz
C (COM)	European Commission
DSG	Datenschutzgesetz (as amended from time to time)
Dako	Datenschutz konkret (law journal)
EC (EG)	European Communities
ECHR (EMRK)	European Convention on Human Rights
ECJ	European Court of Justice
EU-DSGVO	EU-Datenschutz-Grundverordnung
EU-GDPR	EU-General Data Protection Regulation
EP	European Parliament
et seq/seqq	and what follows
f/ff	Folgende/ die Folgenden
Hrsg	Herausgeber
idF	in der Fassung
RGBl	Reichsgesetzblatt
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UWG	Gesetz gegen den unlauteren Wettbewerb
VbVG	Verbandsverantwortlichkeitsgesetz
WKÖ	Wirtschaftskammer Österreichs

Abstract

The right to the protection of personal data is a fundamental right (see Art 8 (2) ECHR).[1] The European General Data Protection Regulation (in further consequence GDPR) makes clear that its main goal is to ensure the fundamental protection of personal freedom, as well as the protection of personal data. It is also a main objective to preserve and strengthen the European Single Market by never restricting free movement of data (see Art 1 GDPR).

In the digital era, where the business model of some multi-million-dollar companies consists of processing data and most companies are dependent on processing data,[2] it is more important than ever to ensure personal data are well protected. The following term paper will, therefore, address the leading question, whether the GDPR is able to ensure a sufficient protection of the personal rights of European citizens. In a vast number of recitals,[3] the GDPR generously mentions the intention to protect personal data. Therefore, it will be closely examined how the mechanism for protecting such data works, and if those mechanisms can ensure the desired protection.

The GDPR entered into force on 25th May 2016 and is fully applicable in all Member States since 25th May 2018. By the time this thesis will be completed, the GDPR will already be fully applicable in all Member States. No further transition period has been provided. Also, the Member States will have already passed additional legislation, which is specifying aspects of how to implement certain procedures. National implementation was needed, because the GDPR requires the Member States to set rules for specific procedures due to a catalogue of opening clauses, scattered across the Regulation. Thus, allows for different laws within the Member States. It is already apparent that the GDPR did not intend to fully harmonise the data protection law. Hence, it can be described as an artificial regulation.[4]

Moreover, this thesis will put a special focus on the measures that companies must take to comply with the Regulation, as well as actions that can be taken against parties not abiding the law. It will be examined how citizens are directly affected by the Regulation and the effect of corresponding laws on data protection. Within the rights of the citizens, however, it will be distinguished between the rights of employees towards their employer as well as the rights customers have against companies they are interacting with. As service providers (i.e. health professions etc. – which often operate as a microenterprise) play an important role in our

[1] See also Recital 1 GDPR 2016/679/EU.

[2] *Christl*, CORPORATE SURVEILLANCE IN EVERYDAY LIFE, 47 ff;

[3] The GDPR consists of 174 recitals, which cover around a third of the Regulation.

[4] *Feiler,* JustIT 2016, 210.

everyday lives, because they significantly contribute to our economy,[5] their situation will also be considered.

Due to the composition of this thesis at an Austrian University and the relationship of the author to Austrian law, special attention is given to the Austrian legislator, and what rules have been established to supplement and accommodate the Regulation.

As the course for which this thesis was written is not a legal course, only indispensable legal information will be provided by the author. In order to ensure the necessary integrity of the work, the issues addressed will be dealt with thoroughly, as well as scientifically and legally correct. To ensure a suitable and uniform citation method, *leg cit* will be used, because it is appropriate for citing Austrian as well as European sources of law.[6] Whereas, when it is needful to do so, certain elements – especially common abbreviations – will be cited in German. To substantiate the work, articles from relevant scientific papers, legal desk books, international jurisdiction as well as legislative elucidations will be used. To cover relevant news, which, among others, emerged during the law-making process of the Austrian legislator, relevant articles from newspapers will be included. If relevant authors have published important information in daily journals, they are also taken into account.

Finally, the findings will be briefly summarised in the conclusion.

[5] More than 70% of all employees are currently working in the third economic sector <http://wko.at/statistik/jahrbuch/2017_k2.pdf>.

[6] *Keiler/Bezemek*, leg cit[3].

1. Historical Development and Introduction to the GDPR

The following chapter will provide a short overview of the development of data protection law on both levels of the European Union as well as the Member States (in this case mostly Austrian regulations will be outlined).

In October 1995 the European Parliament (in further consequence EP) and the Council passed the Data Protection Directive.[7] The legislative act of an EU directive is not applicable on its own but must be transposed into national law by every Member State to which it is addressed. A directive is usually enacted due to an easier process of law. It is able to ensure certain minimum standards while enabling the Member States to provide additional regulations. The easier process of law results in the liberty of the Member States to enact laws on their own and to have just general outlines being given by the EU legislator.

The additional laws can be established by the Member States to their own measure. The necessary standards, however, have to be fully transposed into national law within a given period of time. Otherwise, the parts of the directive that entitle citizens certain rights, become fully applicable and enforceable against the Member State. Furthermore, due to breach of the Treaties, an infringement proceeding can be filed by the Commission. However, when Member States consider it is required to respond to certain national developments, they are therewith free to do so.

The first legislation in Austria considering the protection of data, especially personal data, was established in the year 1978. The DSG 1978 was applicable since 28th November 1978 and, therefore, national data protection law was established around the same century as in other significant countries (i.e. Germany, USA).[8] However, this legislation was rather geared towards prohibiting the misuse of personal data than the regulation of processing data.

Since the early days of data protection law, technologies advanced even faster in even shorter periods of time. Therefore, it was necessary to take the process of modern ICTs into account and pass regulations to ensure sufficient protection of all kinds of data. Also, personal data became a very valuable business part over the years, which made effective protection even more essential. Though continuous developments in the IT-sector enforced the lawmakers to adopt legislation over time, the legislation within the European Communities did not meet the necessary standards that were proclaimed; yet some countries provided adequate regulation

[7] Directive 95/46/EC (Data Protection Directive).

[8] Earliest data protection law in Austria: ErläutRV 72 BlgNR XIV. GP; Implementation: BGBl I 565/1978 “Datenschutzgesetz 1978 (DSG 1978)”.

mechanisms. Therefore, only a year after Austria voted for joining the EU in 1994, the Data Protection Directive was passed, to ensure a coherent data protection law within the Member States of the European Union.

The intention, to set a minimum standard for data protection law undoubtedly was good, but the legislation within the Member States turned out to be everything but coherent. Since every Member State had different legislation with only the core part being standardised by the EU, the new Directive lead to companies, which were operating in the EU Single Market, had to comply with many different laws. Moreover, the citizens usually did not have sufficient legal protection, if at all the national regulations enabled adequate prosecution of the law-breaking parties. That was because the Directive empowered the Member States to choose what mechanisms should prevent the different parties from breaking the law.[9] Those circumstances resulted in rather weak consequences for the law-breaking parties.[10] As a result it was common practice for big companies to accept paying fines instead of complying with the law.

Moreover, the Data Protection Directive should have been transposed into national legislation by 24th October 1998 at the latest.[11] Over the years the Commission has filed infringement proceedings against many Member States like Austria, Germany and Hungary for instance, for not having fully transposed the necessary laws into national legislation or having softened regulations over time. Many Member States were delinquent in incorporating the Directive into national law. The Austrian legislator for instance, passed the DSG 2000 on 29th July 1999,[12] and it was applicable on 17th August 1999; over a year after the Directive demanded the Member States to establish the necessary laws. The German legislator passed the corresponding BDSG on 18th May 2001, because of an infringement proceeding through the Commission.[13]

These cases depict the problems that arise when the European legislator passes bills, which on the one hand are important for the protection of personal rights; on the other hand, are not fully applicable on their own or require the Member States to pass comprehensive legislation. Although the number of infringement proceedings is declining over the years, the statistics show that Member States still get delinquent incorporating directives into national legislation.[14]

---

[9] In line with Art 24 Data Protection Directive 95/46/EC, Member states "*shall adopt suitable measures to ensure the full implementation of the provisions of [the] Directive*".

[10] In line with § 52 Abs 1 DSG 2000, administrative legal punishment of up to 25.000 € could have been set.

[11] Recital 69 Data Protection Directive 95/46/EC.

[12] Implementation in Austria: DSG 2000 BGBL I 165/1999 – (Datenschutzgesetz 2000).

[13] Implementation in Germany: BDSG BGBL I S 904 – (Bundesdatenschutzgesetz).

[14] <ec.europa.eu/internal_market/scoreboard/_archives/2014/07/performance_by_governance_tool/infringements/index_de.htm>

This is a development that does not provide the necessary legal certainty for the EU citizens but can be circumvented by the EU legislator by passing regulations instead of directives. This is exactly what was accomplished with the GDPR. To prevent Member States from getting delinquent while transposing directives, the EU legislator chose to enact the GDPR in the legislative act of a regulation.

An EU regulation is fully applicable by itself and usually does not need to be transposed into national legislation. However, the GDPR allowed the Member States to lay down certain rules based on opening clauses through their own measures, which will be regarded further down below. Therefore, for the GDPR to grant sufficient protection, the Member States had to pass complementary laws. These complementary regulations were passed by the Austrian legislator recently trough the Datenschutz-Anpassungsgesetz 2018,[15] which put the DSG 2000 out of force and the new DSG 2018 (which is referred to as DSG from now on) into force. The latter is applicable since 25th May 2018. Further on, before the DSG was applicable, a few aspects regarding the DSG itself and other corresponding laws were modified in a last-minute law-making through the Datenschutz-Deregulierungsgesetz 2018.[16] The latter was criticised, among others, claiming to have softened the regulation mechanism of the GDPR, because of the regulation that desists from imposing administrative penalties for first-time infringers.[17] The concrete regulation, as well as possible consequences will be regarded further down below.

All in all, it was a much-needed development to ensure data protection law is coherent within the EU and provides a certain minimum standard, with the addition to allow citizens to take legal actions against law-breaking parties.

[15] BGBL I 120/2017.

[16] IA 189/A AB.

[17] DSGVO: Österreich weicht europäischen Datenschutz auf, Der Standard 25.04.2018.

2. Conceptional Definitions and Scope of Application

As well as previous legislative acts, the GDPR contains a large number of definitions relating to the subject of data. These definitions involve different types of data (i.e. health, biometric or genetic data) as well as definitions for different natural and legal persons. Due to a more broadly approach on how different types of data can be processed, the GDPR uses a vocabulary that is partly new to the data protection law or has gotten a different meaning over time. The following paragraphs will abstract some of most relevant definitions according to the GDPR.

The definition of *personal data* was inherited from the previous Data Protection Directive. It describes information that can be matched directly or indirectly to a natural person (the latter is also mentioned as a *data subject*)[18] by either a precise identifier or general social, economic or demographic characteristics (see Art 4 (1) GDPR). However, information that can no longer be matched to a single individual, is *pseudonymised data* (see Art 4 (5) GDPR).

Processing data by means of the GDPR, is every automated action that involves manipulating data. This reaches from collecting the data, making it available, structuring it, joining data and finally destruction of the data. (see Art 4 (2) GDPR).

A *filing system* is in line with Art 4 (6) GDPR a collection of structured personal data that is accessible by identifiers.

Third party describes a natural or legal person or a government agency, which is not the data subject or the processor itself but processes personal data under the authority of the controller or processor (see Art 4 (10) GDPR).

The *controller* is the natural or legal person or government agency, who alone determines the means and purposes of data to be processed (see Art 4 (7) GDPR). This can be a company for instance, which needs certain information about the customers interacting with the company. Therefore, the company determines which data are processed in what way. The *processor* is in line with Art 4 (8) GDPR any natural or legal person or government agency, who processes data on behalf of the controller.

Consent means the freely given approval by the data subject to process predefined data in a predefined way (see Art 4 (11) GDPR).

[18] Therefore, the GDPR only sees natural persons as data subjects. Conversely, legal persons' data will not be protected. The same is also mentioned in Art 1 GDPR.

2.1. Material Scope of Application

The material scope of the Regulation involves personal data that are processed at least partly automated. In general, the GDPR only regulates the processing of data in a digital form. Data, which are processed manually, are only covered when they are part of a filing system or are likely to form a filing system (see Art 2 GDPR). However, judicial records or judicial archives that contain personal data and/or are part of a filing system are excluded.[19] Also operations concerning national security are not regulated (see Art 2 (2) subparagraph a GDPR), as well as actions taken by security services (see Art 2 (2) subparagraph d GDPR). Moreover, data being processed for solely private purposes or unstructured data collected without automated means are also excluded from the Regulation.

2.2. Territorial Scope of Application

According to Art 3 GDPR the Regulation covers the processing of data through a set of activities, when either the controller or the processor have an establishment in the EU. The processing, however, does not have to take place in the EU. Therefore, companies that do have an establishment in the EU but process the data from elsewhere, also have to comply to the Regulation. Another territorial connecting factor even broadens the scope of application because even processing data through controllers or processors that are not established in the EU, can be regulated under two preconditions. The first one being that the data subject in the Union was offered goods or services even if no payment was required. The second precondition is that the behaviour of the data subject (both the subject and the behaviour must be connected to the Union) is to be monitored.

[19] Recital 15 GDPR 679/2016/EU.

3. Effect of the Regulation on Companies

The following chapter outlines how the GDPR affects companies. When necessary, it will be distinguished between larger companies, which often operate as multinationals, as well as small companies, which can easily struggle adopting broad regulations. In addition to the effects of the GDPR itself, certain interesting aspects of national data protection law will also be discussed.

3.1. Necessary Measures that have to be Adopted

Contrary to the systematics of former data protection law, the GDPR mostly defines the goals that are to be reached and only provides certain specific measures that have to be implemented by controllers and processors. In other words, the GDPR liberalised the data protection law by giving the recipients more freedom while just defining the material goals to be achieved and only certain necessary formal requirements.[20] Therefore, many companies considered the realisation of adequate data protection mechanisms as intricate and confusing. Some due to the fact that responsible persons unwantedly overfulfilled the regulation in order to comply with the GDPR in all cases to avoid sanctioning with severe consequences designated for infringers. Because the sanctions were insignificant, others have not implemented former data protection law to the extent it was required. Therefore, these companies had more effort complying with the Regulation than those companies that already had sufficient protection in the first place.

The following chapter is going to enumerate a list of the most relevant measures that have to be implemented and how such implementation can be done to avoid violations against the GDPR.[21] Since the national legislators have already passed legislation to concretise under what circumstances which actions are penalised, the main standards and the anticipated measures will also be dealt with.

3.1.1. Implementation of a Data Protection Compliance Program and a Protection Officer

In line with Art 24 (2) GDPR the controller has to take a minimum of organisational precautionary measures to ensure appropriate data processing. Such appropriate measures are establishing *data protection policies*.[22] The controller defines what goals must be achieved

[20] *Kofler-Senoner*, Compliance Management für Unternehmen Rz 898.

[21] *Feiler/Forgó* in Feiler/Forgó, EU-DSGVO 1.

[22] *Feiler/Forgó* in Feiler/Forgó, EU-DSGVO 20.

within his data protection as well as the possible commission of a protection officer. The data protection policies contain the organisational structure the controller operates within, as well as the types of data that are to be processed. Furthermore, the data protection policies also have to contain information on how the data are processed (i.e. how long data are stored) and what countermeasures against malpractice are taken.

To protect personal data, besides organisational measures the GDPR also requires implementing technical measures. In line with Art 25 GDPR, data protection by design and data protection by default can be mentioned.

Data protection by design (see Art 25 (1) GDPR) demands to minimise the amount of data collected. The controller has to realise the principles of data protection (see Art 5 and 6 GDPR) by implementing technical measures, which only allow for lawful data processing. When the data subject does not consent for the data to be stored, the storing of the data should be technically prevented. Also, pseudonymising data as early as possible, is a necessary technical measure. Moreover, only eligible persons should be able to obtain data from the controllers' database. Considering health professions, where sensitive data of patients is usually stored on a computer next to the reception, data protection by design can mean to secure the computer technically and physically against possible actions that can lead to patients' data being leaked or stolen.

Data protection by default (see Art 25 (2) GDPR) obliges the controller to set standard rules, which should only collect data that are necessary for the purpose for which they are collected; always having in mind to only allow for a minimum of data being processed – data that are not necessary to perform a contract, therefore, may only be processed with the data subjects' consent.[23] Social networks for instance, must set the standard privacy settings to a maximum level of protection to ensure that user data are only available if the users intended to share their data.[24]

A *data protection officer* (see Art 37 (4) GDPR) has to be designated, either when national law requires for designation, or the business objective is solely processing data, or the controller or processor is a public authority, or the core activity of the processor or controller is to process sensible data from criminal convictions and offences. The data protection officer has to advise the processor or controller in data protection matters according to the GDPR. However, in line

[23] See chapters 3.1.3 and 3.1.4.

[24] The wording of the Art 25 (2) GDPR, however, only includes the controller, not the processor. Meaning that the GDPR does apply a different benchmark whether one is in charge of what data are processed (controller), or only gets the order to process data in behalf of the controller (processor).

with Art 39 as well as Art 83 (4) GDPR, the data protection officer cannot be sanctioned with penalties according to the GDPR. His field of action is only counselling; the penalties when violating the designation of the data protection officer or misinformation by the data protection officer, are aimed towards the processor or controller.

3.1.2. Records of Processing Activities

In general, every controller and processor are in line with Art 30 (1) GDPR required to maintain a *record of processing activities*. The record has to be made available to the supervisory authority when it is demanded. Data subjects, however, have no right to examine the record. Though, some companies are not obliged to maintain the Record if, for example, they are employing less than 250 persons and only unless sensible data are processed. The maintaining of the record can also remain undone when the processing of data cannot harm the data subjects and the data are only rarely processed. Therefore, most employers will have to maintain the record of processing activities, since lots of information regarding the employees are concerned sensitive data according to Art 9 (1) GDPR,[25] no matter if they are employing less than 250 persons. Since the processing of such data is in some cases even legally required, no consent of the data subject is needed.

The record that has to be maintained specifies information mentioned in the Data Protection Policies. Necessary information i.e. are the name and contact details of the controller or processor and – if available – the data protection officer. The record also has to contain the types of data that are to be processed, the categories of affected persons, the categories of the recipients of the processed data, the duration for which data will be stored and when data are transferred in a third country, the name of the country as well as a documentation according to Art 49 (1) GDPR. Furthermore, the record has to contain a general documentation of already mentioned technical and organisational security measures, like particular information regarding the Data Protection Policies and implemented measures like data protection by design or by default. A well-maintained record may come in handy when a controller or processor is confronted with a charge regarding the implementation of data protection law and, therefore, can prove necessary measures were taken to prevent infringements against the GDPR or national regulations. Also, when civil actions are taken against a controller or processor, the record can be a suitable proof for compliance with the regulations.

[25] Sensitive data according to Art 9 GDPR, are data that relates to racial or ethnical origin, political or religious beliefs, health or socio-economic data etc.; in general, data an employer collects about his employees, is likely to be sensitive data, as data concerning sick-leaves, is sensitive data and regularly collected.

3.1.3. Lawfulness of Processing

The systematic approach to ensure data are protected and processing is kept at a minimum, is realised since the GDPR prohibits the processing of personal data, unless there is an exceptional statement of facts allowing for such processing. For a lawful processing, at least a legal basis has to be applicable. Such a legal basis can be a statement of facts listed by the GDPR or the consent of the data subject itself. As different types of data can be processed (i.e. personal data, special sensitive categories of personal data as well as conviction and offence data), the processing by the controller or processor has to fulfil an exceptional statement, depending on the kind of data processed. Most of the data, however, will be covered by Art 6 GDPR, which lists “normal” personal data.

The lawful *processing of personal data* in line with Art 6 GDPR requires for the processing either the consent from the data subject, or the necessity to perform a contract to which the data subject is a party, or the necessity to comply with a legal obligation by the controller or processor, or the necessity to protect health interests of the data subject or a third, natural person, or a task that is carried out mainly in public interest, or a predominant personal interest by the controller.

The *processing of sensitive data* in line with Art 9 GDPR requires either the consent of the data subject, or the necessity to carry out obligations by the controller related to employment and social security law, or the necessity to protect vital interests of the data subject or a third, natural person even when the data subject cannot give consent, or the processing of membership information from a NPO with political, religious or philosophical orientation, or the necessity to claim charges or exercise or defend legal claims, or the presence of major public health or development interest or the necessity of a purpose that is based on preventive or occupational medicine or the law of the Union.

3.1.4. Consent

As just depicted, the processing of data can either be legitimised by a statement of facts via the Regulation itself or the consent given by the data subject. Whereas processing due to a statement of facts usually pursues goals that are aimed towards a higher personal interest of the processor or public interest, the consent given by the data subject is voluntary. Therefore, when a data subject does not give consent, data can only be processed when another legal basis allows for the processing.

The *consent* given by the data subject has to be made freely, informed and specific to the type of processing that will take place. In assessing whether the consent was given freely, Art 7 (4)

GDPR requires to take into utmost account whether the performance of a contract or a service is conditional to the processing of personal data that is not necessary dependent for the performance of the contract or the service. It is, therefore, prohibited to link the – freely given – consent to the performance of a contract.[26] In other words, not giving consent to the unnecessary processing of data, must not lead to a worse performing contract or no contract at all. However, it is a vastly spread business model to offer a service free of charge, conversely data are processed and sold.[27] Not giving consent to such processing of data would lead to certain companies being unable to offer their service free of charge any longer. A predominant special interest of the controller also has to be taken into account. Therefore, it can be possible to offer two kinds of service models: A free of charge model that conditions for the consent being given and a model where data subjects have to pay for the same service but must not give consent. The customer is free to decide whether he wants to give consent or pay for a service, though it must be clarified. However, to achieve full legal certainty, it has to be awaited if a data subject remonstrates against a controller having implemented such a model and how such a case will be ruled. The prevailing doctrine, however, considers such a constellation admissible.[28]

At the moment the practice shows, depending on the website in question, that some operators do offer a "pay or consent" model,[29] others do not make it that clear, but rather stick to the standard cookie-information instead, disguising the processing of information to the user. As already mentioned, the performance of a contract must not be worsened when not consenting to the processing of data, which clearly could be the case in the "pay or consent" model, since neither paying nor consenting likely leads to no contract at all; though, the consent must be given freely. Forcing the data subject to either pay for the service or click the consent button, probably violates the principle of not linking the performance of a contract to the given consent. However, it will remain questionable until the ECJ disposes such a case, whether the monetary interest of a controller in showing individual advertisements to a user of the controller's website, can qualify as a predominant personal interest which, therefore, cannot be objected by the data subject and also legitimises the processing as no further consent is needed. It may also be argued that not providing a service to parties that have not consented to the terms is not a

[26] Also see Art 7 GDPR „Koppelungsverbot".

[27] Many online newspapers and most social media offer their service free of charge, while processing their users data and selling them to advertising and analysing companies; according to slogan *„When you don't pay for the product, you are the product"*.

[28] *Feiler/Forgó* in Feiler/Forgó, EU-DSGVO 13; *Fellner,* VbR 2018, 84 (86).

[29] Online newspapers like <derstandard.at/> use a "pay or consent" model; others like <nzz.ch/> or <diepresse.com/> use the standard cookie information.

worse performing contract since there was no contract in the first place. Though, Art 7 (4) GDPR also mentions the *"provision of a service",* therefore, denying a service to parties not consenting can be seen as a violation of the principle. However, as already mentioned above it is easily conceivable that the predominant personal interest of the controller or processor in the processing, can qualify as the legal basis for the processing and, therefore, no consent is needed, and an objection can be invalid.

3.1.5. Security of Personal Data

In line with Art 32 GDPR the controller as well as the processor have to implement necessary technical as well as organisational measures to ensure a certain level of data security. It is taken into account that the necessary security measures can differ according to state of the art, the cost of implementation and the nature, scope and purposes of processing. Therefore, smaller companies or small service providers will have to take less effort than companies whose business model consists of processing data or large companies in general. The level of security also depends on the types of data processed. Someone who is exercising a health-profession, therefore, processes lots of sensible data, will have to adopt more thorough security measures than someone who is, for example, a carpenter or a barber.

Adequate security measures can involve, early pseudonymisation of data in the processing process, measures to protect IT-systems that process data, implementation of incident-response measures and regularly evaluating these measures. In practice, ISO standards like ISO/IEC 27001 and ISO/IEC 27002 provide basic guidelines to ensure the security of processing data.[30] Moreover, when new technologies are involved in the processing of data and the processing is likely to yield a high risk for the data subject, the controller must carry out a *data protection impact assessment* pursuant Art 35 GDPR. The supervisory authority, however, may establish a list of processing operations for which no such impact assessment is required.

3.1.6. Privacy Notice

Contrary to measures like the record of processing activities or data protection policies that are designated for mostly internal use,[31] therefore, allowing for proof, when a person concerned claims violation of the GDPR, the privacy notice is addressed to the data subject for information about the processing of data. The information within a privacy notice has to be

[30] *Feiler/Forgó* in Feiler/Forgó, EU-DSGVO 27 f.

[31] Except the request from the supervisory authority in line with Art 30 point 4 GDPR.

displayed in a precise, transparent and easily understandable language. A *privacy notice* (see Art 13 GDPR) always has to contain the information about the controller and the processor, the purpose of processing and the corresponding legal basis, the recipient of the processed data, the time the data are likely to be stored, the existence of rights the data subject has regarding his data, the existence of a right to file a complaint by the data subject and if automated decision-making processes exist, the notice and logic of these processes. Furthermore, a privacy notice can be made under different circumstances, depending on where the personal data are collected.

If the personal data are collected *directly from the data subject*, the same must be informed whether the data collection is necessary or compulsory and what the consequences are when not consenting to the collection.

If the data are *not* collected *directly from the data subject*, the same has to be informed about the type of data to be collected and the source the personal data are coming from; also, whether the providing source is public or private.

When data are collected on a *public website*, a *layered privacy notice* is often used in practice. The first layer should briefly provide the necessary information regarding the data subject, the collected personal data as well as options to obtain further information (via a link for instance). The second layer of the privacy notice should provide a summary of the most important articles of the privacy policy. The third layer should provide the full privacy policy and the complete information. [32]

3.1.7. International Data Transfer

When the controller or processor intend to transfer personal data to a third country or an international organisation, a three-step procedure to ensure the transfer is legally admissible can be brought up. The first step involves data that is neither subject to registration nor subject to authorisation, therefore, can be transferred quite easily. The second step are data that are subject of registration when transferred. The third step are data that are subject to authorisation when transferred. If none of these statements of facts allow for a transferring data in an intended situation, the data transfer is unlawful.[33]

Transfer of personal data that is *neither subject to registration nor subject to authorisation* can be admissible under following circumstances that are related to the data subject itself: the data subject gave consent to transfer the data, the transfer is necessary to fulfil a contract, the data

[32] *Feiler/Forgó* in Feiler/Forgó, EU-DSGVO 16; *Feiler/Forgó* in Feiler/Forgó, EU-DSGVO Art 12 Rz 1.

[33] *Feiler/Forgó* in Feiler/Forgó, EU-DSGVO 33 ff.

are transferred in a public or vital interest, the data to be transferred descends from a public register, the data are necessary to file or defend legal claims. Moreover, the transfer is also admissible when the Commission either decided the third country or organisation can provide an adequate level of protection, or when standard contractual clauses that were issued by the Commission were set between the controller or processor and the recipient of the data transfer, or when binding corporate rules in line with Art 47 GDPR were set.[34]

The transfer of data that is *subject to registration* in line with Art 49 (1) subparagraph 2 GDPR is either admissible when it does not happen frequently, or when the number of data subjects is limited, or when mandatory interest of the controller predominates the interests of the data subject or when appropriate data protection safeguards were established by the processor.

The transfer of data that is *subject to authorisation* is either admissible when appropriate data protection safeguards in line with Art 46 (3) GDPR were established or administrative arrangements between two public authorities include effective data subject rights (see Art 46 (3) lit b GDPR).

3.2. Adverse Consequences when not Complying to the Regulation

Art 83 GDPR provides for the administrative fine that penalises certain misconducts with up to 20m € or up to 4% of the total worldwide turnover, whichever is higher. It is mandated that the penalty set should be *"effective, proportionate and dissuasive"*. This legal norm was the origin of many worries from companies around the globe, since such a high range of sentences is very uncommon when it comes to administrative penalties. Furthermore, awarding such a high fine could lead to severe injuries of smaller companies or ones that are not fully solvent.

The following paragraphs will explore under which circumstances companies can expect penalisation. Also, what degree of punishment is likely to be set as well as what kind of other sanctions can be taken. Since Member States were allowed to set national legislation regarding the sanctions, the rules in question will also be examined.

3.2.1. Non-Monetary Sanctioning by the Supervisory Authority

To ensure, the processing of personal data is in accordance to the GDPR, the supervisory authority has the right to investigate processing activities in line with Art 58 (1) GDPR. The right to investigate empowers the supervisory authority to order the controller or processor to

[34] E 2001/497/EG ABL 2001 L 181.

provide information that is necessary to fulfil the tasks regarding the supervisory authority (see Art 75 GDPR); especially the task to monitor and enforce the Regulation. The supervisory authority is authorised to get access to the premises of the controller or processor and data processing equipment, to further investigate whether the processing is in line with the Regulation.

When it is suspected that an intended processing is not in line with the Regulation, the supervisory authority has the power to issue a warning to the controller or processor (see Art 58 (2) subparagraph a GDPR). The supervisory authority may also educate both controllers and processors on how compliance between the processing operations and the GDPR can be achieved. Moreover, in line with Art 58 (2) subparagraph b GDPR the supervisory authority has the right to issue a reprimand to a controller or processor, when an act of processing already infringed the Regulation. If an infringement already took place, the data subject concerned has to be informed.

In addition to imposing an administrative fine pursuant to Art 83 GDPR, the supervisory authority can impose the limitation of processing of personal data as a further consequence on non-compliance. Furthermore, the supervisory authority may even prohibit the controller or processor from processing data. The supervisory authority, therefore, has a vast number of instruments to investigate and force a (potential) infringer to comply with the GDPR. Even the power to prohibit further processing of data, which is causing the infringer to be unable to operate any longer. These instruments make it reasonable for every controller or processor to follow the supervisory authority's instructions.

3.2.2. Administrative Fine According to GDPR

In concreto, Art 83 GDPR distinguishes two degrees of severity of the infringement with a principle of congruence, while having due regard for the individual case (see Art 83 (2) GDPR). Offences against fundamental principles of the GDPR, like the principle of consent and the lawfulness of processing for instance,[35] can be fined with up to 20m € or, in case the infringer is a legal person, with 4% of the total worldwide turnover, whichever is higher (see Art 83 (5) subparagraph a GDPR). This higher fine is also applicable to offences against the rights of the data subjects, offences against rules to transfer data to a third country and offences for not obeying instructions of the supervisory authority.[36]

[35] See Articles 5 to 7, 9 GDPR.

[36] See Articles 12 to 22, 44 to 49, 58 GDPR.

Offences against other rules of the GDPR can be fined up to 10m € or, in case the infringer is a legal person, up to 2% of the total worldwide turnover, whichever is higher (see Art 83 (4) GDPR). This case covers the majority of the statements of facts mentioned in the GDPR, again with the principle of congruence, while having due regard for the individual case. As noteworthy provisions that can have legal consequences, offences against the general obligations of the controller and processor (see Articles 8, 11, 25 to 39, 42, 43 GDPR) and offences against the obligations of the certification as well as the monitoring body can be named (see Articles 41 to 43 GDPR).

As already mentioned, Art 83 (2) GDPR contains a principle of congruence, which takes into account whether the infringer committed the violation negligently or deliberately. Furthermore, the supervisory authority has to determine whether the infringer has set adequate countermeasures to prevent such violations.[37] As already mentioned above, the more thoroughly the controller or processor kept the data protection policies or the records of processing activities, the easier it will be to prove the abidance of data protection law to the supervisor authority. A controller who barely implemented precautionary measures, will consequently have a problem to justify the processing taken place, therefore, infringing the Regulation. Depending on the severity of the infringement, the fine has to be adapted to every single case.

It has to be mentioned that the administrative penalty only depicts the maximum possible penalty. Therefore, in most cases a lower fine will likely to be inflicted. However, the GDPR mandates the fine to be *"effective, proportionate and dissuasive"*. Additionally, the Member States were allowed to set certain rules to encounter specific national circumstances and made use of that opportunity. How these rules have affected the national legislation, will be examined down below.

3.2.3. Monetary Sanctioning Mechanism According to the DSG

In line with § 30 DSG the supervisory authority can inflict a legal punishment when an infringer violated regulations set by the GDPR or the DSG itself. In case the violation was committed by a legal person, the infringer must either be a body of the legal person or representative that has legal power within the legal person. Legal punishment can also be imposed when the infringement is due to a lack of supervision by the bodies of the legal person and the infringer acted on behalf of the legal person.

[37] Such adequate measures can be obligations like data protection by design and data protection by default (both mentioned in Art 25 GDPR), which should have been implemented by the controller.

However, there are a few national exception clauses where no legal punishment is set, respectively the supervisory authority refrains from imposing such punishment. In line with § 30 (5) DSG, the supervisory authority does not set legal punishment against public authorities (see opening clause Art 58 (3), 83 (7) GDPR). Also, according to the existing principle of congruence, the supervisory authority can refrain from imposing legal punishment against infringers and *issue a warning instead*. In line with § 11 DSG and Art 58 (2), (3) GDPR, the supervisory authority acts upon a proportionality principle. Meaning an infringer committing an offence for the first time, probably will not face consequences, depending on whether the infringement occurred negligently or purposely. The latter is likely to carry a penalty because such kind of behaviour must not be tolerated.

According to Art 83 (9) GDPR, the Member States had to provide the Commission with the national legislation regarding the sanctioning mechanism by 25th May 2018 at the latest. That is because the Commission acts as the guardian of the contracts and investigates whether the Member States operate within the law of the Union.[38] In consequence, the national legislation was partly criticised vigorously because data activists and political analysts feared the sanctioning mechanism of data protection law to become insufficient.[39] However, WKÖ's general secretary states that the principle of "issuing a reprimand instead of a fine for first time infringers", leads to a great relief amongst market participants.[40] Also, the relevant EU-commissioner stated that the legislation of the Austrian lawmaker will be checked thoroughly, whether it is in accordance with the rather strict sanctioning mechanism of the GDPR. It is argued that the sanctioning mechanism does not allow such a regulation because it is conclusive, and it is feared that infringers will hardly face a penalty at all. If such a regulation is contradictory to EU law, an infringement proceeding against Austria could be filed by the Commission. Also, the supervisory authority and courts would have to apply the regulation of the GDPR and ignore a contradictory national regulation. That is because of the primacy of application of Union law – overruling national and constitutional legislation. Though, legal certainty can only exist, when certain national regulations have been subject to a critical scrutiny by the Commission.

[38] The TEU as well as the TFEU provide the legal basis of the actions taken by the EU (no matter if it is law-making or prosecution); Member States violating these terms, for example when disobeying law of the Union, may face infringement proceedings according to Art 260 TFEU.

[39] DSGVO: Aufweichungen sorgen für Kritik, Der Standard 26.04.2018.

[40] WKÖ begrüßt Klarstellungen und Verbesserungen durch das Datenschutz-Deregulierungs-Gesetz 2018 <ots.at/presseaussendung/OTS_20180420_OTS0196/wkoe-begruesst-klarstellungen-und-verbesserungen-durch-das-datenschutz-deregulierungs-gesetz-2018>.

However, the GDPR itself mandates a principle of congruence, and a due regard to the circumstances of the individual case. As already mentioned above, Art 58 GDPR mandates the possibility for the supervisory authority to issue a warning not only when a controller or processor are likely to violate the Regulation, but to issue reprimands when a violation already occurred (see Art 58 (2) b GDPR). At this time, it is difficult to make a point whether the national regulation is compatible with the GDPR or not. Both sides have reasonable arguments. On the one hand, the GDPR mandates fines to be *"effective, proportionate and dissuasive"* (see Art 83 (1) GDPR), on the other hand, the corrective power to issue a reprimand by the supervisory authority does not seem necessary any more when a penalty already has been inflicted because a reprimand should be issued before an infringer is fined.

Regarding the vagueness of some formulations, the intention of the Austrian legislator, however, can be comprehended. The GDPR requires controllers and processors to comply with regulations that can be fined with a very high amount. As already mentioned above, the outcome – the protection of personal data – was set, but the parties concerned had to implement the measures to a degree they thought that was sufficient to ensure the intended protection. The practice shows that there is no completely safe way to implement data protection law, while having due regard to the cost of the implementation. It is, therefore, possible that an unintentional violation of the Regulation can occur, although the implemented protection mechanism was sufficient in most cases.[41] That is why, each case has to be handled individually and all the measures set by the infringer have to be evaluated, whether they were sufficient to grant reasonable protection or not.

In some constellations it seems necessary for the supervisory authority to ensure the protection mechanism is fundamentally capable of achieving the desired protection and, therefore, issuing a warning seems adequate but it might not necessary to impose a legal penalty. However, in cases were a controller or processor purposely or negligently provided a protection mechanism that is obviously insufficient, only issuing a warning might not be an adequate sanction. The practice will show how the supervisor authorities cope with the set sanctioning mechanisms and whether the concerns of softening data protection law were appropriate.

The regulation *excluding public authorities* from receiving legal penalties was also subject to criticism.[42] That is why it has to be mentioned, that actions taken by the state always have to comply with the legality principle (see Art 18 B-VG), meaning there has to be a legal basis for

[41] Recently, Facebook unintentionally made 14m private user posts public, while implementing a new software, which was compromised by a bug <kleinezeitung.at/lebensart/multimedia/5442947/Oeffentliche-Privatsphaere_Neue-Datenpanne-setzt-Facebook-weiter>.

[42] DSGVO: Aufweichungen sorgen für Kritik, Der Standard 26.04.2018.

every action taken by the state or his acting bodies. Furthermore, there is a comprehensive control possibility by either the data subject itself or political parties as well as legal protection against unlawful actions taken by the state. Therefore, public authorities can only process data when a legal basis allows for the processing in question, in default whereof, a damaged party can file a claim in line with § 1 et seqq AHG.[43] However, the public authority will not face administrative fines according to the GDPR or *in concreto* the DSG itself. Such fines would have to be paid to the Member State whose supervisory authority imposed the legal penalty. This would lead to a peculiar situation, since the federal state would investigate, fine and make a payment to himself.

However, it is a common regulation to exclude public authorities from certain sanctions such as penal sanctions (see § 1 (3) sub-paragraph 2 VbVG). This is due to the fact, that public authorities always have to comply to the legality principle and can be monitored by the state. Their bodies, however, can be sanctioned via penal law when abusing their authority. Therefore, excluding public authorities from the sanctioning mechanism according to the GDPR, does not mean they can act upon the law since their bodies can always be prosecuted. Therefore, the national regulation, excluding public authorities being sanctioned according to Art 83 GDPR, is clearly incorporated into existing national legislation.

3.3. Legal Persons as Data Subjects

As already mentioned above, in line with Art 1 GDPR only natural persons can be data subjects. Therefore, personal data related to legal persons cannot be protected by the Regulation itself. However, since the right of protecting personal data is a fundamental right (see § 1 DSG 2000, Art 8 (2) ECHR), the Austrian legislator enacted parts of the former legislation, which also covered legal persons as data subjects, as a constitutional right.[44] Over the course of the legislative adoptions, which transposed the necessary parts of the GDPR into national legislation,[45] the Austrian legislator wanted to put these clauses, awarding legal person the position of data subjects, out of force. Since these clauses were constitutional clauses and the legislator did not manage to obtain the required majority of votes to change constitutional law,[46] Art 1 DSG 2000 which, among other clauses, determined legal persons as data subjects, will be applicable further on (see Art 1 DSG).

[43] § 1 (3) subparagraph 2 VbVG idF BGBl I 112/2007 allows for sanctioning legal persons with penal law.

[44] See Art 1 DSG 2000.

[45] Datenschutz-Anpassungsgesetz 2018 as well as the Datenschutz-Deregulierungsgesetz 2018.

[46] Art 44 B-VG requires half of the members of the parliaments attendance and two thirds of their votes for changing constitutional law.

However, the fact that legal persons are still considered data subjects according to the DSG, does not mean the same mechanisms the GDPR provides for natural persons are also applicable on legal persons. In fact, the GDPR consistently mentions natural persons when determining certain regulations. Therefore, legal persons can, in the best case, only be protected by § 1 DSG.

Not covering legal persons as data subjects according to the GDPR, brings a great relief to data processors and controllers, as they do not have to extend their established mechanisms on personal data which are processed from companies they are interacting with. Moreover, the WKÖ appreciated the regulation for it provides legal certainty.[47] The natural persons that stand behind those companies, however, are fully covered by the mechanisms of the GDPR.

[47] WKÖ begrüßt Klarstellungen und Verbesserungen durch das Datenschutz-Deregulierungs-Gesetz 2018 <ots.at/presseaussendung/OTS_20180420_OTS0196/wkoe-begruesst-klarstellungen-und-verbesserungen-durch-das-datenschutz-deregulierungs-gesetz-2018>.

4. Effects on Citizens of the European Union

The following chapter illustrates what rights people concerned have, no matter whether it is the right of a customer against an entrepreneur or a website operator, or the right of an employee against the employer. In line with Art 12 GDPR, the controller has to take appropriate measures to provide information concerning those rights.[48] When demanded by the data subject, the information has to be provided in an easily accessible form; either in a written statement or electronically, when demanded, even orally. Furthermore, the information has to be presented in an easily understandable language. However, the controller may ask for prove of identity by the data subject, to ensure information is only provided to an eligible person. Moreover, Member States are allowed to set national legislation regarding the rights of data subjects, taking into account national and public security as well as public interests, national defence and general prevention of criminal offences as well as prosecution of offences.

4.1. Entitlements of the Citizens

4.1.1. Right of Information and Right of Access

In Line with Art 15 GDPR, the data subject hast the right to demand and receive information from the controller, whether or not personal data concerning the data subject are processed. If personal data are processed, the operator has to provide information regarding the purpose of the processing, the types of data involved, the duration the data are saved, if data are transferred to recipients, those recipients or categories of recipients, if data were collected from a public register, the type of register and the fact that the data subject has the right to have the data rectified and deleted as well as the right to restrict the processing of data. If data are processed through an automated individual decision-making system, the information concerning the type of logic involved to the system has to be provided.

If data are collected directly from the data subject and the same has not received the following information yet, Art 13 GDPR demands the controller to provide the name and contact data regarding the controller himself and whether a processor or data protection officer exists. The contact information regarding the previous cases has to be provided as well. Furthermore, the controller has to provide information regarding the purpose and the legal basis of the data processing, whether the processing is due to a legal basis or due to performance of a contract, the duration the data are stored and what circumstances affect the duration. Also, if data are transferred to a third country or other recipients, further information regarding the recipients or

[48] The Rights of the Data Subject are mentioned in Art 12 to 23 GDPR.

the third country has to be provided. Furthermore, the controller has to provide information regarding the rights of access to and rectification as well as the deletion of the data. If data are processed via an automated decision-making system, information regarding the logic has to be provided.

If data are not collected directly from the data subject, the same information as mentioned in Art 13 GDPR has to be provided. Additionally, the controller has to provide information regarding the source, the data was obtained from, and whether or not the data was shared with another recipient.

4.1.2. Right to Rectification and Right to be Forgotten

In line with Art 16 GDPR, the data subject has the right to have the controller rectify or complete personal data concerning the data subject. Furthermore, Art 17 GDPR entitles the data subject to have data deleted when one of the following alternative preconditions apply: further storage of the data is not necessary anymore, the data subject revokes the given consent and no other legal basis allows for storing the data, the data was unlawfully processed in the first case or the controller is obligated by law to delete the data. If data are processed by a processor, it can be demanded to delete the data, taken into account the available technology to erase the data is available. The last case can occur, when a user in an online forum posts a user comment and that content is shared by other users or the processor or controller himself. This can lead to an uncomfortable situation for the processor since it is hardly possible to browse through the entire internet to erase all the data subjects shared comments. Therefore, among others the GDPR takes the right to free speech and a public interest into account when a data subject asks for erasing certain data. Also, sensitive data regarding an employment contract that has to be stored by law, may not be deleted on behalf of the data subject.

4.1.3. Right to Restriction of Processing

In line with Art 18 GDPR, the data subject has the right to demand restriction of processing personal data, when one of the following alternative preconditions apply: the personal data are not complete or correct and the processor had the chance to rectify the data, the processing is unlawful but the data subject does not want to have the data erased, the processor no longer needs the data but the data subject is eventually pursuing legal claims or the data subject objects to processing the data but the controller claims a predominant personal interest in processing the data. Restriction of processing entitles only the processor being able to store the data, but no further processing is allowed.

4.1.4. Right to Data Portability

A data subject has the right to obtain the personal data from a controller or processor, when the processing is due to consent given by the data subject or due to performing a contract with the processor, and when the processing is done via an automated mechanism (see Art 20 GDPR). The data subject is then able to convey the personal data to another processor.

4.1.5. Objection to Automated Processing and Direct Marketing

According to Art 21 (1) GDPR, the data subject has the right to object the processing of personal data that are not necessary to perform a contract. The objection, however, may not be regarded when the controller demonstrates a predominant personal interest in the processing. Furthermore, the data subject has the right to object the processing of personal data by the means of profiling when the profiling is based upon a legal basis[49] but does not legally or significantly affect the data subject, and the controller cannot demonstrate a predominant personal interest in the automated processing.[50]

Whereas Art 21 (1) GDPR determines the inadmissibility of the processing in general, Art 21 (3) GDPR determines the inadmissibility of a certain purpose. Objecting to automated decision making by the means of direct marketing pursuant Art 21 (3) GDPR, does not lead to a weighing of interests, therefore, the controller or processor cannot not process data for such purposes any longer.[51]

4.1.6. Objection to Profiling

In line with Art 22 GDPR, a data subject has the right to object to individual automated decision-making and profiling if the data subject is legally or substantially affected by the processing. However, when the processing is either necessary to perform a contract, or a consent was given for the processing, or law of the Union allows for the processing, the objection is invalid, and the further processing is lawful.

4.2. Legal Enforcement of the Citizens' Rights

To provide a sufficient protection mechanism, it is of utmost importance to ensure that people concerned have an easy access to legally enforce their given rights. Therefore, the GDPR provides several judicial remedies that can be exercised by the data subject.

---

[49] For a legal basis for profiling, see Art 6 (1) point e and f GDPR.

[50] *Feiler/Forgó* in Feiler/Forgó, EU-DSGVO Art 21 Rz 2 ff.

[51] *Feiler/Forgó* in Feiler/Forgó, EU-DSGVO Art 21 Rz 6.

The first being the option to *lodge a complaint* with the supervisory authority in the respective Member State, when a data subject claims that certain processing of data infringed the Regulation (see Art 77 GDPR). The supervisory authority then has to review the case and act in accordance to the sanctioning mechanism of the GDPR when necessary. The opportunity to lodge a complaint, is the least sophisticated remedy for the data subject since the supervisory authority is obligated to do all the necessary investigation and sanctioning. The second option is the right of the data subject to a *legal remedy against the supervisory authority*, either when the data subject is not informed within three months about the progress of a complaint according to Art 77 GDPR, or the complaint did not get handled by the supervisor authority. The third option is the right of the data subject to a *legal remedy against a controller or processor*, when the data subject claims that processing data concerning the data subject, infringed regulations of the GDPR (see Art 79 GDPR).

The last two remedies, however, require legal counselling at least since they lead to legal proceedings. Therefore, it is an unalterable clause in the GDPR for data subjects to be represented by a public, not-for-profit body, whose statutory objectives are to ensure the protection of data subjects' rights and personal freedom (see Art 80 GDPR).

4.2.1. Civil Lawsuit for Damage Claims

In accordance with Art 82 GDPR, any person has the right to file a lawsuit for compensation against a processor and controller, when claiming that the processing of personal data infringed the Regulation and lead to damage. As *Zankl* states, the wording of Art 82 GDPR entitles *any person* to file claims for damages, not only data subjects. This case may be applicable, when the rights of children got violated, therefore, in addition to the data subject, relatives may also file claims for damages.[52] This remedy can be exercised in addition to a complaint with a supervisory authority since the latter may only lead to an administrative penalty.

To ensure the claim for damages can be exercised in a reasonable manner, the GDPR allows the lawsuit to be brought to court either where the controller or processor has an establishment, or where the data subject has a habitual residence (see Art 79 (2) GDPR). As some companies might only have an establishment in one Member State or even no establishments in the EU at all, this regulation unburdens the enforcement of citizens' rights immensely.

Moreover, to facilitate the provability of asserted claims, Art 82 (2) GDPR mandates a reversing body of proof. Meaning, a controller or processor that gets sued for damages, has to prove not

[52] *Zankl,* ecolex 2017, 1150 (1151).

to be responsible for the cause. On the one hand, that mechanism facilitates the civil procedure for claims for damages for the data subject but on the other hand, it burdens the controller or processor, which have to prove they are not culpable for the damage arisen. A way to prove a controller or processor is not responsible, can be a well implemented protection mechanism according to the requirements of the GDPR.

4.2.2. Combined Lawsuit and Complaint with Supervisory Authority

In line with Art 80 (2) GDPR, it is up to the Member States to set national legislation for combined lawsuits against controllers or processors, or combined complaints with the supervisory authority. A combined complaint is detached from a concerned data subject, allowing a not-for-profit organisation to claim a controller or processor infringes the GDPR.[53]

The Austrian legislator, however, did not make use of this possibility. Therefore, only natural persons, if applicable legal persons, can take these remedies. However, the German legislator implemented the bespoken mechanism into national law. In consequence, this can lead to an uncertain situation, because a German not-for-profit organisation can file a combined complaint with the German supervisory authority against an allegedly infringing company located in Austria. The GDPR mandates the complaint to be forwarded to the Austrian supervisory authority,[54] which would not accept such a complaint lodged by an Austrian not-for-profit organisation. At this point it is unclear how the Austrian supervisory authority has to handle the claim. Not handling the claim, however, can lead to a legal remedy against the supervisory authority by the German not-for-profit organisation pursuant to Art 78 GDPR. On the other hand, handling the complaint would lead to discrimination against the Austrian not-for-profit organisation as the latter is not allowed to file a combined lawsuit. This case depicts that desirably the GDPR would have regulated such cases by setting less opening clauses.

[53] The preliminary ruling for a combined complaint vs Facebook filed by data activist *Max Schrems* for instance, was disallowed by the ECJ; see In Case C-498/16.

[54] Art 56 (1) GDPR determines a “one-stop-shop” principle, meaning, there is one lead supervisory authority that is obligated to handle a certain case; other supervisory authorities, however, may assist the lead supervisory authority.

5. Further Difficulties and Implementation in Third Countries

Since the European market with over 500m potential customers is a highly profitable market for companies around the world, this chapter will depict the difficulty when having strict regulations within the EU, which also affect companies from third countries. As the act of law-making usually includes a trade-off between comprehensive guidelines to cover the intended facts and circumstances as well as the constraint of personal freedom, further difficulties regarding the GDPR itself or actions concerning the GDPR will be discussed.

5.1. Data Protection Law in Third Countries

According to Art 3 (2) GDPR, the Regulation is also applicable to the processing of personal data of data subjects located in the EU, by a controller or processor not located in the EU, when the processing is related to offering goods and services to data subjects or monitoring the behaviour of data subjects. The offering of goods or services must not yet carry a payment, therefore, even the already bespoken case of operating a public website by a controller not located in the EU, is covered by the GDPR. As a consequence, a controller or processor, no matter where they are established, or where subsidiaries may exist, have to comply to regulations set by the GDPR, in default whereof, they can face consequences.

The first problem that occurs, is that only addressed Member States had to establish a supervisory authority that is empowered with investigative and sanctioning mechanisms discussed above. Furthermore, the national supervisory authorities can only operate within the boundaries of the Member State itself (see Art 57 (1) GDPR). Therefore, international law enforcement regularly faces administrative difficulties pursuant to the principle of sovereignty. However, the GDPR mandates every controller or processor located only in a third country, to designate a representative in the Union (see Art 27 GDPR). According to Art 50 GDPR, the Commission and the Member States take appropriate measures to enable the international cooperation regarding data protection law. As *Tretzmüller* correctly states, the Union is aware of the problem regarding international law enforcement, but does not provide a solution, rather than formulating a desired outcome.[55] Concluding, an infringer that has a subsidiary in the EU would face fines according to Art 83 GDPR, the international infliction of administrative fines could only be enforced when the third country, in which the infringer operates, approves for the enforcement. Such an approval would have to be negotiated with every concerning third

[55] *Tretzmüller,* Dako 2018, 8 (9).

country, meaning that the Member States alone will have a much worse negotiating position than the whole EU represented by the Commission.

However, besides the administrative penalty, the possibility to file claims for damages exists. Therefore, the latter could be the incentive to motivate a controller or operator to implement the regulations of the GDPR. According to private international law as well as the Clause 9 of the Standard Contractual Clauses for Processors, the infringement is to be judged upon the law of the state where the infringement took place.[56] Unfortunately, the international enforcement of the claim may again be the factor for damaged parties to desist from pursuing their rights. A person concerned will have to file the action against the infringer at the legal domicile of the infringer, but the case will be judged upon law of the Union or national law. Lodging a claim in a third country can come along with unforeseen risks and costs depending, among others, on procedural law. Therefore, the GDPR enabled the Member States to allow not-for-profit organisations to accumulate complaints and file a combined lawsuit. The importance of such an instrument can facilitate legal enforcement.[57]

Another point also mentioned by *Tretzmüller* – maybe the most important point – is whether companies can meet up with the customers' ideas for trust in their personal data.[58] In some cases, therefore, it might not be necessary to file sophisticated lawsuits. The public image of a company, which violates data protection law, can lead to severe economic consequences. The bigger the company, the more likely it is information regarding violations of data protection law are made public. It is also more likely that either the government will begin to intervene, or market shares are lost in favour of smaller participants. [59]

All in all, the mentioned sanctioning mechanisms and civil actions are a first but suitable step and might probably lead to controllers and processors from third countries to comply to at least the basic principles of the GDPR.

5.2. Spamigation from Private Actors

Since the GDPR facilitates the law enforcement regarding damaged data subjects or simply the violation of the Regulation, it was feared that the same mechanism may be abused by

[56] See § 13 (2) IPRG – (Bundesgesetz über das internationale Privatrecht, private international law); Commission Decision C (2010) 593, Clause 9 Standard Contractual Clauses (Processors).

[57] *Tretzmüller,* Dako 2018, 8 (9).

[58] *Tretzmüller,* Dako 2018, 8 (10).

[59] The EP for instance questioned Facebook CEO Mark Zuckerberg regarding Facebook's relation to data protection law, even signalising to regulate the business model when the compliance is poor <multimedia.europarl.europa.eu/en/meeting-with-mark-zuckerberg-at-european-parliament_6501_pk>.

private actors to admonish a controller or processor regarding the supposedly unlawful processing of data or a not fully existing compliance with the GDPR (i.e. the implementation of a privacy notice etc.).[60] The German jurisdiction for instance, enabled market players to file certain claims or complaints via competition law.[61] Basically, it would be welcome to enable a company, whose competitor violates data-protection-law, to file a claim according to competition law. However, it has yet to be ruled, whether claims regarding violations of the GDPR can also be filed by private actors upon competition law. The practice, however, shows that some market players have already stared to send out such adhoratory letters by the day the GDPR was applicable. Such letters are addressed to potential infringers and threaten to bring in a claim for damages and to lodge a complaint, unless the spamigator is paid a certain amount for his expenditure.

Such spamigation, however, has been mostly listed in Germany so far and might not be likely to expand to other countries because the mentioned peculiarity in the German jurisdiction. It also has to be mentioned that a too liberal enforcement mechanism can lead to a state of utter mutual surveillance and even abuse of law, which might not be desirable. Nevertheless, pursuing a claim for damages or a claim against an anti-competitive actor is permissible, it is more than questionable whether legislation that allows for private actors to admonish others and exploit the Regulation is reasonable.

[60] DSGVO: Die Abmahn-Maschinerie ist angelaufen, 30.05.2018 <heise.de/newsticker/meldung/DSGVO-Die-Abmahn-Maschinerie-ist-angelaufen-4061044.html>.

[61] An adhortatory letter can be filed in line with the German § 3 a UWG, since jurisdiction paved the road to private actors enforcing those letters (KG, 22.09.2017 - 5 U 155/14).

6. Prospect of Data Protection Law

Data protection law within the EU is a multi-step-process. It all started with the Data Protection Directive[62], which was supplemented over the years with the "e-Privacy-Directive"[63] and the "cookie-Directive"[64]. The recent development, the GDPR, was the biggest leap so far, as it was the first regulation to intend to fully harmonise data protection law to a certain minimum standard among the Member States. The next big step within the EU will be the "e-privacy-Regulation", for which the Commission already introduced a proposal in January 2017.[65] Originally it was intended, for both the GDPR and the "e-Privacy-Regulation" to be fully admissible on 25th May 2018, but the latter faced too much of a headwind in the European Parliament, hence the wording of the regulation has to be revised. Therefore, it is expected for the "e-Privacy-Regulation" to enter into force in early 2019 and be applicable at least a year later.

The subject matter of the "e-Privacy-Regulation" will be much more concrete than the general approach of the GDPR. Users should have the full authority whether to decide – among others – if cookies are set or not. Hence web-browsers are likely to act as "gatekeepers" where users can decide to consent for setting cookies. Furthermore, every communication channel should take a part in the subject of data protection. Excessive web-tracking should, therefore, not be possible anymore. The same applies for unwanted electronic-communication which, however, is already banned in many Member States. Furthermore, a basic principle realised in the GDPR will also be used – though tightened – in the "e-Privacy-Regulation"; specifically, the prohibition to process data, unless there is a legal statement of facts in the Regulation that allows for the processing in particular.[66]

However, the exact wording of the "e-Privacy-Regulation" must still be clarified. It is to hope that together with the GDPR the data protection law within the EU reaches an acceptable level, while having due regard to the fast developments that are distinctive to the ICT-sector. As *Wiebe* states, it will be a most sophisticated undertaking to cope with the developments, such as automated transport and artificial intelligence, which enable matching user profiles to natural persons, therefore, possible threatening data protection and personal freedom.[67]

---

[62] Data Protection Directive: Directive 95/46/EG.

[63] E-Privacy-Directive: Directive 2002/58/EC.

[64] Cookie-directive: Directive 2009/136/EC.

[65] Proposal of the Commission for the e-Privacy-Regulation: COM (2017) 10 final.

[66] <wko.at/branchen/information-consulting/werbung-marktkommunikation/ePrivacy-Verordnung.html>.

[67] *Andreas Wiebe, Datenschutz*-Grundverordnung erfordert neue Regeln für Mensch und Maschine, Der Standard 12.03.2018.

7. Conclusion

As the wording of the General Data Protection Regulation already implies, its main goal was to implement a set of minimum standards for data protection law among the Member States of the European Union. The implementation process within the single Member States, regarding persons concerned that had to implement the regulation, turned out to be quite different. That is because some Member States already had comprehensive regulations regarding the subject of data protection, while others did not. By no means the GDPR intended to implement a complete amount of regulations, but rather plays a fundamental role in the development of comprehensive data protection law within the European Union. It is expected for the “e-Privacy-Regulation” to enter into force in 2019 and to be applicable in all Member States about a year later. Therefore, to reach thorough coverage in most of the subjects of data protection law, it will be relevant how the “e-Privacy-Regulation” copes with the concrete subjects in question, like telecommunication and e-privacy regarding tracking, etc. Moreover, the ECJ will have to rule certain cases that will come up over time, because the GDPR formulated some aspects rather abstractly.

The GDPR takes up the issue of data protection law in general, while not including too narrow subjects. A general mechanism for the principles of data protection was established, as well as a mechanism for sanctioning the infringers of those principles. The general protection mechanism consists of fundamental principles of data processing; especially under what circumstances such processing is allowed. Basically, the processing of data is prohibited, unless as statement of facts given by the GDPR or the consent of the data subject allows for the processing in question. Furthermore, controllers and processors had to implement – depending on the possible amount of processing that is likely to take place and the kinds of data that are to be processed – a more or less comprehensive protection mechanism that allows for easy investigation by the supervisory authority and documentation of the processing in general.

Further, the legal enforcement of infringements of data protection law was refined. Persons concerned now have a catalogue of sufficient instruments to legally proceed against potential infringers. The least sophisticated way is to lodge a complaint with the supervisory authority. The same has to pursue the complaint, and if necessary, inform the lead supervisory authority, which has to take further measures. Besides lodging a complaint, persons concerned can legally proceed against the supervisory authorities for when they are not informed in time or the complaint was not handled at all. At last, when damage was suffered due to processing of data by a controller or processor, the persons concerned have the right to file claims for

damages. As a facilitating circumstance, it is up to the controller or processor to prove he is not responsible in any way for the damage caused. The liability of both the controller and processor leads to the intrinsic motivation to mutually check whether each interacting party meets the standards of the GDPR. Complying to the above-mentioned protection mechanism can indicate whether a controller or processor meets the standards, therefore, is a trustworthy party to interact with. Also, to prove someone is not responsible for damages caused, the compliance to the protection mechanism will be taken into account.

Unquestionably, the sanctioning mechanism was the part of the Regulation discussed most often, due to the amount of the maximum penalty. However, it was rarely discussed under what circumstances an infringer will face what amount of penalty. Surely, due to the fact that the GDPR mandates the fine to be – among others – dissuasive. However, the concrete sanctioning mechanism according to the GDPR leaves a lot of questions open. Nevertheless, it was recognised to judge each case individually, while having regard to the measures the infringer set to prevent the infringement in the first place. Due to the abstract and in some cases unclear formulation of the Regulation, the Austrian lawmaker was criticised for his legislation to issue a reprimand to first time infringers instead of a fine – when it seems proportionate. As already mentioned above, the criticism – among others brought up by the commissioner of justice – regarding this regulation would not take a long time to occur, because the GDPR mandated the Member States to educate the Commission concerning national legislation. Therefore, it has yet to be ruled whether this national regulation is in line with the GDPR, and companies will not face excessive penalties; even when infringing the Regulation for the first time.

It also has to be mentioned that data protection law within the European Union is at held at a much higher level than in other comparable regions like America or the Asian region for instance. One of the main difficulties of the GDPR is to guarantee the same protection to European citizens within the EU, as to European citizens who are interacting around the globe. It shows that especially international operating companies, which do not have an establishment in the Union, therefore, cannot be subject of administrative penalties, do need intrinsic motivation to guarantee data protection meets the high standards required. This can either be achieved through the Commission negotiating administrative assistance with the third countries concerned or when an infringement already took place, via legal action taken by the persons concerned. Besides the costs and risks of legal actions taken in a third country, private international law states the national law of the persons concerned – in this case besides national legislation the GDPR – to be applicable. Therefore, persons concerned do have a good chance in getting compensation from infringers located in third countries.

All in all, it can be said that the GDPR manged to fulfil its intended goal – to set general rules for data protection law across the European Union. However, it is up to the companies concerned whether they comply with the regulation, which – when looking at the possible adverse consequences – seems reasonable. It also has to be mentioned that in times, where information is so rapidly transferred as today, information about breaches of data protection and data privacy reaches nearly all the existing and potential customers at any time. Therefore, it is in the best interest of market participants to comply to the regulations, in default whereof, market forces might change to their disfavours. Also, the GDPR and the ubiquitous debates regarding data protection and data privacy managed to establish a certain amount of awareness around the citizens; despite it is a customer who was flooded with privacy notifications or a body of company that had to implement mechanisms mandated by the GDPR. Another important point achieved by the GDPR is that every person concerned, no matter if it was a controller, a processor or a data subject, more or less thoroughly had to deal with the subject of data. Therefore, it can be said that the GDPR was a step in the right direction, however, it was not the last step. Although, there is a continuous need to monitor whether the protection mechanism is still sufficient for new technologies that are entering our everyday lives.

Table of Resources

Legal Sources

Judicature/EU/Commission

Commission 05.02.2010, C (2010) 593

Commission 02.08.2001, C (2001) 1593

Commission 10.01.2017, COM (2017) 10 final

Judicature/EU/ECJ

ECJ 25.01.2018, In Case C-498/16, *Maximilian Schrems/Facebook Ireland Limited*

Judicature/Germany

KG Berlin 22.09.2017 - 5 U 155/14

Legislation/EU

Directive 95/46/EC Official Journal 1995 L 281/31 - Data Protection-Directive

Directive 2002/58/EC Official Journal 2002 L 201/37 - E-Privacy-Directive

Directive 2009/136/EC Official Journal 2009 L 337/11 - Cookie-Directive

Regulation 2016/679/EU Official Journal 2016 L 119/32 - General Data Protection Regulation

TEU (Lisbon)

TFEU (Lisbon)

Legislation/Germany

BDSG BGBL I S 201 idF BGBL I S 904

UWG RGBL S 145 idF BGBL I S 254

Legislation/Austria

B-VG BGBl 103/1931 idF BGBL I 22/2018

DSG 1978 BGBl I 565/1978

DSG 2000 BGBl I 565/1978 idF BGBl I 132/2015

DSG 2018 BGBl I 565/1978 idF BGBL I 120/2017

IPRG BGBl I 119/1998 idF BGBl I 87/2015

VbVG BGBl I 112/2007 idF BGBl I 26/2016

Literature

Legal Desk Books

Keiler/Bezemek, leg cit[3] (2014)

Kofler-Senoner, Compliance Management für Unternehmen (2016)

Feiler/Forgó in Feiler/Forgó (Hrsg), EU-Datenschutz-Grundverordnung (2017)

Law Journals

Feiler, Öffnungsklauseln in der Datenschutz-Grundverordnung - Regelungsspielraum des österreichischen Gesetzgebers, justIT 2016, 210

Tretzmüller, Der globale Anwendungsbereich der DSGVO - warum die DSGVO auch in Drittländern umgesetzt werden sollte (muss), Dako 2018, 8

Zankl, Unklare DSGVO-Haftung, ecolex 2017, 1150

Other Journals

Christl, CORPORATE SURVEILLANCE IN EVERYDAY LIFE (2017)

Andreas Wiebe, Datenschutz-Grundverordnung erfordert neue Regeln für Mensch und Maschine, Der Standard 12.03.2018.

DSGVO: Österreich weicht europäischen Datenschutz auf, Der Standard 25.04.2018

DSGVO: Aufweichungen sorgen für Kritik, Der Standard 26.04.2018