Norbert Bernsdorff*

"Data Protection Law" of the European Union**

1. Data Protection and the European Commission's Requirements of 17 June 2022

I would like to start my presentation with a question: Does the European Commission – EU Commission - complain about deficits in Georgian data protection at all? If so, are they substantial or does the existing data protection law just need a "fine-tuning"?

The opinion of the EU Commission of 17 June 2022 is ambivalent: The Commission demands - firstly - "to equip the...Personal Data Protection Service with resources to its mandate" and - secondly - "to ensure its institutional independence" (page 17). Elsewhere in her report (page 10), she states that "the Personal Data Protection Service...still needs to prove its efficiency and independence". That is all the opinion contains.

In my first presentation I already referred to the so-called Copenhagen criteria that an applicant country must fulfil. One of these criteria is the "acquis criterion" – from the French word "acquis communautaire". According to this, a candidate state must adopt the entire body of rules and regulations of the European Union (EU), meaning integrate several 10,000 pages of legal texts into its national law and implement them into corresponding administrative and judicial structures. What the "acquis" comprises in the area of European data protection law results from the "Association Agreement" between the EU and Georgia from 2014. There, in an "Annex" (I and XV-b) to Article 14 and Article 327 of the "Agreement", reference is made to data protection law of the Council of Europe and now obsolete - no longer valid - law of the EU... one more reason to look at the current, completely redesigned legal situation in the EU today.

2. Adoption, Implementation, Enforcemen

First of all, a question of understanding needs to be clarified: If a candidate country has to adopt the EU rulebook, how is this done technically?

The EU has no legal means to carry out the integration of its law into the national law of the candidate state itself. Like accession, this is done voluntarily by the candidate country. There are three stages in the integration of EU law: "adoption", "implementation" and "enforcement", meaning "law enforcement". For the first two stages, the terms "transposition", meaning "conversion of law", and "application", meaning "application of law" are also commonly used. The integration of EU law into national law is regularly an apolitical process. There will be fewer so-called "veto players" here; because political disputes in the candidate state have already taken place before, namely before the application for membership was submitted.

What does the term "compliance" mean in this context?

---

* Professor at Philipps University of Marburg (Germany); Retired Judge at the Federal Social Court of Germany.

** The publication represent the text of the report presented by the author within the framework of public lectures held in the scope of cooperation of Ivane Javakhishvili Tbilisi State University Law Faculty and Institute of Administrative Sciences. The event was dedicated to the issues of Georgia's integration with the European Union.

"Compliance" or "non-compliance" refers to the phase after accession to the EU. It refers to whether a member state complies with the adopted law of the EU completely or not at all, only incompletely or late. This is monitored by the EU Commission and the Court of Justice of the EU (CJEU). The keyword here is: Infringement proceedings!

Is the integration of EU law at the first level - "adoption" or "transposition" - an automatic process?

Yes! - The technical instrument for this is the "accession" of the candidate country. This takes place through the accession agreement (under international law) with all other EU member states. From the date of accession, the candidate country becomes a party to all treaties of the EU in their current version. All EU legislation concluded on the basis of these treaties up to the date of accession automatically becomes binding on the acceding state. The EU legislation take precedence over any national law. This is explicitly recognised by the candidate country in the accession agreement (under international law).

What does this mean for EU data protection law? - With accession, this also "grows" into the national legal order as a priority right!

In this lecture, I do not want to compare Georgian and European data protection law with each other; my aim is not to look for successes or deficits of a future "adoption" or "transposition". I cannot do that at all, because I do not have the so-called progress reports, the "Association Implementation Reports" which have been produced annually since 2016. These are held by the EU Commission and the competent authorities in Georgia; however, I am neither an employee of the EU nor an official representative of the member state Germany. To make such a comparison is the task of TAIEX, the "Technical Assistance and Information Exchange" Group of the EU Commission, which should have been in Georgia since last year.

So what is my task today?

I want to give an overview of

- firstly: the so-called primary law and the so-called secondary law of the EU, here above all the General Data Protection Regulation.
- secondly: current areas of conflict under data protection law in the EU
- thirdly: new legal developments and
- fourthly: the requirements of European law for effective data protection control.

3. The European Union's Primary Data Protection Law

All EU action is based on the European treaties. These treaties between EU member states set out objectives and rules for the EU's institutions as well as the decision-making processes and the relationship between the EU and its member states. The treaties are the basis for EU law and are referred to as "primary law" in the EU. The legislation based on the principles and objectives of these treaties is called "secondary law" and includes regulations, directives, decisions, recommendations and opinions.

a. Primary and Secondary Law

Since 2009, when the Lisbon Treaty came into force, the legal framework for data protection in European primary law has been the Charter of Fundamental Rights of the European Union – European Charter of Fundamental Rights, in this case Article 8. Although the primary law level also includes Article 8 of the European Convention on Human Rights and a Council of

Europe Convention from 1981, the focus of my presentation will be on Article 8 of the European Charter of Fundamental Rights.

In order not to let my lecture get out of hand, I will also limit myself to the presentation of secondary data protection law. Although there is now a wealth of secondary law regulations and directives in the EU, I will focus here only on the General Data Protection Regulation, which has been in force since 2018. It is now the central legal institution for the protection of personal data in Europe and has led to a radical change in data protection law in the EU.

b. Article 7 and Article 8 of the European Charter of Fundamental Rights

The protection of personal data is an essential aspect of the protection of private life. The latter is regulated in Article 7 of the European Charter of Fundamental Rights. Because it considered it so important, the EU has dedicated a separate, special provision to data protection - in this different from the European Convention on Human Rights - namely Article 8. The fundamental right to data protection must be respected by EU institutions, bodies and agencies, as well as by each EU member state when implementing European law.

What does "implementation of EU law" mean in this context?

First of all, it should be noted that EU member states are not bound by EU fundamental rights if they exclusively apply their national law; then national fundamental rights apply. The case is different when EU law - for example a European directive - is implemented. This also happens through national "legal acts" of the EU member states; however, these are only "interposed" and ultimately represent an "extension" of EU sovereignty. National courts have to apply European fundamental rights in addition to national ones. This sounds complicated, but when thought through, it is simple.

c. Essential Baselines

I do not want to keep you long with dogmatic subtleties. Therefore, only a few hints at this point:

Article 8 of the European Charter of Fundamental Rights is an enforceable right. Like any classical fundamental right, it is above all a right of defence against the state and its authorities. However, Article 8 also obliges to ensure the protection of personal data by private parties. The fundamental right to data protection thus has a so-called third-party effect.

In the area of data protection, Article 8 of the European Charter of Fundamental Rights contains statements on the scope of protection and on when an interference with the right to protection of personal data is justified; furthermore, Article 8 requires the establishment of "independent bodies" to monitor compliance with data protection law. Whether the holders of fundamental rights also include legal entities has not yet been clarified in the EU.

The fundamental right to data protection has a special feature - and this is the last thing I will say here: It is "reverse engineered"! - In German it is referred to as "norm-engineered".

What does that mean? - It means that the fundamental right to data protection is predetermined at all levels by the respective current European secondary law - in this case the General Data Protection Regulation. The content of Article 8, which is part of the primary law of the EU, is therefore derived "one-to-one" from the content of the secondary law, which is at a

normative level lower. If secondary law changes, the fundamental right also changes. This is a result that is actually not compatible with the principle of the so-called hierarchy of norms.

What is the EU's motive behind this?

The development in the field of processing personal data is very dynamic. The intention was to make the fundamental right to data protection "open to the future". Secondary law can be adapted to such processes more quickly and easily than primary law.

4. Secondary Law: General Data Protection Regulation

Since May 2018, the General Data Protection Regulation – abbreviated GDPR - has been in force at secondary law level. It replaced a European directive that had existed since 1995, the so-called Data Protection Directive (95/46/EC).

a. The Differences Between an EU Regulation and an EU Directive

What impact this has on European data protection only becomes clear when one knows the differences between an EU regulation and an EU directive:

Directives are limited to prescribing a certain result for EU member states. The achievement of this result, on the other hand, is left to the member states themselves; they have to transpose directives within certain deadlines through their own national legal acts. In contrast, EU regulations are directly and immediately binding on all EU member states and not, like a directive, only with regard to a result to be achieved.

What prompted the EU to replace the former Data Protection Directive with a Regulation?

With the former Data Protection Directive, all EU member states had the same legal basis. However, they could determine the implementation of data protection themselves.

Accordingly, there was a considerable imbalance in the level of data protection in the individual EU member states. With the introduction of the GDPR, which is directly and immediately binding on all member states, this imbalance should be eliminated.

At this point, one more remark! - Because the fundamental right to data protection in Article 8 is being filled out by the secondary-law GDPR - I have just reported on this - the Regulation is being elevated to the rank of a fundamental right, so to speak. However, this is disputed in European legal dogmatics.

b. Principles and Key Points of the General Data Protection Regulation

I would now like to familiarize you with some of the central contents of the GDPR. I do not claim to be exhaustive. Nevertheless, it should become clear what level of data protection the EU has been aiming for since May 2018.

(1) On the One Hand: No Limitation of Data Protection to Risky Information Processes

The GDPR does not limit its application only to risky information processes such as "profiling", "scoring" or the use of so-called "artificial intelligence". Rather, it applies universally. And rightly so; because ubiquitous computing has paved the way for "big data" at all levels. Data power in the hands of the state and in the hands of private individuals is growing. Individuals,

however, are supposed to retain control over their own data and thus the ability to exclude third parties from collecting or using this data. They should be able to obtain information about the collection of their personal data and to work towards the deletion of data. Because personal data is now collected everywhere, such data must be protected not only in critical areas but also in everyday life.

(2) On the Other Hand: No "Brake Block" for Economic Development

Recently, the data protection commissioner of a federal state in Germany resigned from his service. He belongs to the "Free Democratic Party (FDP)" in Germany, which primarily represents business and economic interests. The reason he gave was: The European data protection is anti-business. It puts the EU economies at a disadvantage in the international competition. Data protection fails to recognize that personal data also has an economic potential, an economic value.

A widespread prejudice must be cleared up here! - The GDPR does not prohibit the use of personal data in the economy, it actually protects it. Article 1 of the GDPR explicitly safeguards the "free movement of personal data". This may therefore neither be restricted nor completely prohibited for reasons of data protection. Data processing in the economy is therefore not taboo; it only has to comply with the processing conditions regulated in Article 6 of the GDPR. To ensure that European data protection does not “stifle” digitalization in the economy - file-based and “artificial intelligence” applications - supervisory authorities and courts in the EU have an important task: They must not overemphasize data protection or even "make it absolute", but rather must appropriately balance the interests of the economy against the protection of personal data.

Current example: Because it considers data protection to be absolute in this way, the European Court of Justice prohibits the use of software for video conferencing systems if it comes from outside Europe - in this specific case, the USA: Zoom, Microsoft Teams, Cisco Webex etc. But, as long as there are no corresponding technical alternatives in Europe, the European economy needs them.

(3) Scope of Application — Establishment Principle, Market Place Principle, Data Transfer to Third Countries

The situations to which the GDPR applies are governed by Article 2 of the Regulation. In principle, this applicability is comprehensive; the GDPR is binding for both public and non-public bodies, meaning also for private parties. However, it does not apply to police activities and law enforcement. A separate directive applies here, but it is structured similarly.

The GDPR presupposes automated data processing. This is to be understood broadly; Article 2 is "technology-neutral" in this respect. This does not include purely analogue storage of data and purely manual data processing – on index cards, paper forms, etc. Exceptionally, the handling of personal data in the family sphere is not covered by the GDPR. This is called the household privilege.

Does the GDPR apply only in the EU or worldwide because of the global flow of data across all borders?

In our networked world, the processing of personal data hardly knows any technical boundaries. Therefore, the application of the GDPR must be geographically limited. Because all

member states of the EU are obliged to provide the same level of data protection, it naturally applies geographically without restriction in the EU. However, particular caution is required in the case of data processing by non-European companies; data transfers to countries outside the EU also give rise to suspicion. The level of data protection is often significantly lower there. The GDPR solves these problems in Article 3 with the so-called establishment principle and the so-called market place principle. Non-European Companies with an establishment in the EU are bound by the Regulation, but a mere letterbox in the EU is not sufficient for this. If such a company does not have an establishment in the EU, it is nevertheless bound by the GDPR if it operates in the internal market of the EU. Therefore, Google and Facebook – Meta - are subject to European data protection law.

What about personal data in the cloud? Is there a "loophole" here? – No! - In such a case, it depends on where the server is located.

If data is exported to third countries, an adequate level of protection must be provided there. That of the EU - often referred to as the "data protection gold standard" - is frequently not achieved. According to Article 45 of the GDPR, such a data transfer must be allowed by the EU Commission in a so-called adequacy decision. I will come to the data protection agreements with the USA later.

(4) General Prohibition with Reservation of Permission, Legal Permissions and Consent

To the European data protection law, the following basic principle applies: The starting point is a general prohibition with a reservation of permission.

What does this mean? - The processing of personal data is generally prohibited unless it is permitted by law or the owner of the data - the "data subject" - gives his or her prior consent. The EU has thus agreed on a preventive approach that gives high priority on the protection of personal data.

Article 6 of the GDPR regulates when the processing of personal data is legally permitted. I do not want to go into too much depth here; therefore, only very briefly! There are five grounds for permission: Data processing is lawful when it concerns the conclusion or fulfilment of contracts; after the contractual relationship has ended, however, personal data must be deleted again. A data processing may also take place if a vital interest of the "data subject" is affected, for example in the fight against epidemics - Corona - or natural disasters. Processing is also permitted in the case of a legitimate interest of the person processing the data. This is the case if the "data subject" is his customer in business transactions or is employed by him; such a legitimate interest is, for example, the prevention of fraud by the "data subject". Finally, the performance of public tasks is sufficient for data processing. The European case law on this is now almost unmanageable.

As an alternative to legal authorizations, the prior consent of the "data subject" may justify the processing of personal data. Here too, just a few remarks: Consent must be voluntary, and the "data subject" concerned must know the meaning of his or her consent. Minors up to the age of 14 cannot give effective consent as a rule. Subsequent consent to the data processing - called "authorization" in legal terminology - is not sufficient to justify it.

(5) The Classification of data

Personal data can be classified. Some data can be obtained from generally accessible sources - from telephone and address books, from the internet, others have to be obtained in a complicated way. Some data are important for the integrity of a person - they are sensitive, others are not. In most cases, generally accessible and less sensitive data are less essential from the perspective of the "data subject". Because Article 6 of the GDPR does not differentiate here, Article 9 of the Regulation contains stronger protection for qualified data. This includes, for example, data on ethnic origins, political and religious beliefs, health and sexual orientations.

What does European data protection provide for so-called public figures - politicians, judges, actors, etc.?

There is a strong public interest in persons who are prominent, that is to say who have a certain degree of notoriety. Within the so-called public sphere - in the case of public appearances or public statements - the data protection of these persons is restricted. In this sphere, personal data may be collected, for example photos may be taken, without their consent. If this area is left and it concerns the so-called private or even intimate sphere - domestic sphere and family - the same protection exists as for unknown persons.

Article 9 of the GDPR then applies without restrictions.

(6) Information Duties, Rights of Access, Rectification, Deletion and Blocking

As a novelty compared to the previous legal situation, the GDPR provides for numerous rights for data holders in Articles 12 to 17. They are intended to help enforce the right of defense under data protection law. This begins with the duty of information of a processor of personal data who in this way must "open" the "black box" of his processing. This also applies above all in cases of a "data breach", when data flow in an uncontrolled manner. Protection instruments that require the "data subjects" to take the initiative themselves are a right of access and a right of rectification against the processor of the data.

Particularly noteworthy is the right of the "data subject" to have his or her data deleted in Aricle 17 of the GDPR. This has made a name for itself in recent years as the "right to be forgotten". The European Court of Justice has clarified this right in four decisions against Google since 2014. If personal data are not deleted, they can be blocked for users.

(7) Data Protection "in Advance": Data protection "By Design" and "By Default"

Let me now address one last point:

A ground-breaking innovation of European data protection law is also that it wants to take preventive action and prevent breaches of data protection "in advance". Until now, the only legal instruments available in this area were the regulations on so-called data economy or data minimization. Now, the sparing use of personal data is to be supported through technical or organizational precautions - "data protection by design" - or default settings - "data protection by default". The first area includes, for example, so-called pseudonymisations, the second area so-called patterns. Violations of these principles are punishable by fines.

c. Excursus: Law of Georgia on Personal Data Protection

As part of my preparations, I only looked very briefly and superficially at the Law of Georgia on Personal Data Protection, which I found on the homepage of the "Personal Data Protection Service". I assume that this is still valid. From the latest amendments to the law in December 2016 it appears that the former European Data Protection Directive (95/46/EC) still served as a model for this. However, as just discussed, the GDPR is now setting new priorities. Two things struck me: On the one hand, the Georgian law largely exempts the media from the application of data protection law when they collect data for journalistic purposes.

On the other hand, the law - as I read it - is also applicable to analogue data processing - "processing of data by non-automatic means".

5. Current Areas of Conflict in the European Union

As I have already stated in my presentation, the right to protection of personal data is not a "super fundamental right". It is not granted completely without limits or conditions. For example, it can collide with the - also protected - right of internet users and media companies to obtain information. But it can also come into conflict with the freedom of art, science and research. This is then called a "multipolar conflict". In these cases, the different interests must be weighed against each other and balanced: so-called practical concordance.

a. Data Protection and Freedom of Information - Internet Users and Media Companies

There is always an emotional debate in the EU about the relationship between data protection law and freedom of information; the latter is a manifestation of freedom of expression. Why this is so, is easily explained: The "data subject" wants to retain control over his or her personal data. As a rule, internet users and media companies usually want to invade privacy as much as possible.

Question: Does the GDPR contain a solution to this conflict?

Yes! - However, the EU does not balance these conflicting interests itself. Instead, Article 85 of the GDPR assigns this task to the EU member states. They must enact legal provisions for this purpose. Article 85 is a so-called opening clause, which gives the member states a "margin of appreciation". However, the GDPR does give one instruction: Paragraph 2 of the aforementioned provision obliges the member states to regulate "derogations" and "exemptions" from the GDPR if the data processing serves journalistic purposes. Background: Such a "media privilege" was and still is widespread in the national law of the EU member states.

Just for interest: What measures by the member states can be considered here?

One instrument, for example, is to oblige platform operators to set up filter systems - so-called upload filters. However, an upload filter system that is too far-reaching and lacks contours, with the consequence of "over blocking" even content that is not problematic from a data protection perspective, is likely to violate freedom of information.

b. The Permanent Problem of "Data Retention"

The issue currently attracting the most media attention is the so-called data retention. This refers to the obligation of telecommunication companies to store location and traffic data of

users of their services without concrete reason and over a long period of time. The aim is to make it easier for the security authorities to fight serious crime and international terrorism.

The so-called data retention has already written legal history: Originally, a European directive had required EU member states to store location and traffic data "in advance". After initial reluctance on the part of the European Court of Justice, the directive was declared invalid in 2014. The reason: The directive disproportionately restricted the protection of personal data.

In the following period, the European Court of Justice reviewed national laws on so-called data retention. In doing so, it has remained true to its original line, according to which such a retention represents a disproportionate encroachment on data protection law. Nevertheless, the EU member states have repeatedly enacted regulations on so-called data retention. In total, the European Court of Justice has handed down seven rulings against Germany, Estonia, France, Ireland, Austria and Sweden in the last ten years. In the political arena, alternatives to so-called data retention are now being discussed: the so-called login trap and a so-called "quick freeze" procedure. The so-called login trap allows the automated storage of the IP addresses of criminals without technical leading to a mass surveillance. With the so-called "Quick Freeze" procedure security authorities can have location and traffic data "frozen" at the provider. They can then access it with a court order.

c. Application of So-called Artificial Intelligence: ChatGPT

The use of so-called artificial intelligence is in principle not a subject of regulation under the GDPR. Nevertheless, it can pose problems in terms of data protection law.

One example is the text robot "ChatGPT"; "GPT" stands for "Generative Pre-Trained Transformer". It has been on the market since November 2022 and is currently attracting a lot of attention worldwide. In order to classify it in terms of data protection law, one needs to know something about how it works: "ChatGPT" is supposed to generate texts based on user input. It is based on so-called artificial intelligence that has been trained with a huge amount of data. It is true that individual users can protect their personal data by not entering it into the tool. However, the main data protection problem lies elsewhere; it concerns the text robot's database. There is a risk that the training material also contains data with a personal reference. In case of doubt, their processing can lead to a "data breach" for which the user is held responsible. The fines of the GDPR are high.

d. Transfer of Personal Data to the USA

I have already mentioned that cross-border data traffic with third countries - for business and trade - is necessary, but risky for data protection. According to Article 45 of the GDPR, such a data transfer requires a so-called adequacy decision by the EU Commission. This also applies to the transfer of personal data to the USA.

Since the "Edward Snowden" case and his surveillance by the US intelligence service, trust in American data protection in the EU has been – more or less - lost. EU citizens can also be observed in the USA, for example when they send messages via the US network Facebook - Meta.

In 2000, the EU Commission concluded a data protection agreement with the USA, called "Safe Harbour". It regulated compliance with data protection principles to which American companies had to commit. This was intended to "raise" the level of data protection in the USA

to that in Europe. Five years later, the European Court of Justice declared this "Safe Harbour" agreement invalid. The Court referred to the USA PATRIOT Act, which allowed American security authorities to access personal data without the consent of the "data subject".

In the following years, a new agreement was negotiated with the USA, the "EU-US Privacy Shield" agreement. Although it provided for improvements in data protection, it was still not sufficient for the European Court of Justice. In 2020, the Court also found this - and the EU Commission's so-called adequacy decision - to be unlawful. What this means is clear: It is currently still illegal under data protection law to transfer certain personal data from the EU to the USA. For information, the EU Commission is currently in the process of drafting a third EU-US data protection agreement.

6. The Future Development of the Data Protetion Law – Regulatory Frenzy of the European Commission

I now want to say a few words about legal developments in the EU!

Data is everywhere and increasing at a breathtaking pace. The hereby associated benefits for business, science and administration are euphorically welcomed. Data has become a key advantage for the economy. At the same time, the disadvantages for the protection of personal data resulting from a free flow of data are lamented. Both views are sometimes irreconcilably opposed to each other. However, there is agreement that Europe needs a legal framework beyond the GDPR.

Since 2020, the EU Commission has been working on a so-called European strategy for data; with this, it wants to enforce a single market for data that is as free as possible in the interest of the EU's economies and its global competitiveness. To this end, it has made proposals for four European regulations: With the first, a "Data Governance Act", it wants to create "data intermediation service providers", who, as neutral bodies and without economic self-interest, collect data and, if certain legal requirements are met, distribute it to interested parties. This principle is called "data altruism". In this way, it wants to limit the power of data monopolists such as Apple, Amazon, Facebook – Meta – and Google. The second proposal for a "Data Act" goes even further: It should regulate who owns the data that users of networked devices – such as surveillance systems or autonomous vehicles - generate themselves. So far, only the providers of such systems can access them, but not the users.

But the EU Commission is not leaving it at that!

It is also planning a "Digital Services Act". This aims to regulate online platforms; it is aimed at internet providers, cloud services, app stores and social media. Such companies must take measures to detect and remove illegal products and content at an early stage. Violations face fines of up to 6 percent of annual turnover. Finally, a "Digital Markets Act" is in preparation. It targets only the big "gatekeepers": Apple, Amazon, Facebook - Meta, Google and Microsoft. According to this, providers of messenger services and social media are to be obliged to offer so-called interoperable services. A WhatsApp message should then also be received via "Threemo-Messenger" and "Signal". Companies like Apple also have to grant access to other app stores. I don't want to go into this further here. Some of these regulations have already come into force.

Because data protectionists no longer know where "up and down" is in the digital jungle from all the initiatives of the EU Commission, they are calling for new, more effective instruments of data protection. One of the instruments is the creation of a "data ownership regime". As with the ownership of property, this should regulate who has the authority to

dispose over and to use personal data. Comparisons are drawn with copyright law. Should people be able to sell and transfer their data? - Another objective is pursued by the “Charter of Fundamental Digital Rights of the European Union" proposed by data protection experts. It is intended to supplement the European Charter of Fundamental Rights, here Article 8, and to protect personal data even better through specialized fundamental rights. A revolutionary concept!

7. Data Protection Control – “Data Protection Law Compliance” and External Supervisory Authorities

Effective data protection needs monitoring. No right can be effective if there is no monitoring of whether it is respected. The right to protection of personal data is particularly sensitive because individual violations often go unnoticed. A data protection control must take this into account.

How is this issue dealt with in EU law?

If one looks at primary law, that is to say Article 8 of the European Charter of Fundamental Rights, it hardly provides any answers. It is true that paragraph 3 of the fundamental right to data protection requires the establishment of "independent bodies" to monitor obedience to the protection of personal data. However, the legal meaning of this requirement is disputed in the EU. Only a few experts see it as a genuine institutional guarantee.

The GDPR is more detailed here. It is "two-track" and systematically distinguishes between "internal control" and "external control". According to this, the task of monitoring is initially assigned to the processors of data, the authorities and companies. According to Article 37 of the GDPR, they are obliged to appoint a data protection officer. He or she is independent within the authorities or companies. It is true that the data protection officer does not have to be involved in the leading decisions of the authorities` or companies` policies; however, he or she has free access to every processing operation and is to be involved in decisions on this. It is interesting to note that such an obligation for "data protection compliance" did not exist under the law of the Data Protection Directive (95/46/EC) in force until 2018.

Could European law leave it at this mere self-regulation?

The answer is: No! - It is true that internal control by such data protection officers makes sense; for they know the processes in and the structure of their authorities or companies well and can therefore carry out systematic and regular controls effectively. However, such internal controls are often also characterized by hierarchies and dependency relationships. For this reason, the GDPR also relies on a concept of "external control" by external data protection supervisory authorities.

What do one need to know about this "external control" at the level of the EU member states? - I will only briefly outline the system of data protection supervision in the GDPR:

According to Article 51 of the GDPR, independent supervisory authorities are to be provided for. "Independent" means "completely independent". The European Court of Justice understands this to mean that the data protection supervisory authority has to be remote from the government, meaning the supervisory authority must not be subordinate to a ministry. Excluded from the supervisory activities are - because of the "media privilege" - the media, also the churches and, according to Article 55 of the GDPR, the courts. Background: This is to ensure the independence of the judiciary. The main task of the data protection authorities is classical supervisory activity with the possibility of imposing fines of up to 10 million euros. The

supervisory authorities are also appeal bodies. Appeals against their decisions can be lodged with the courts.

To conclude my presentation, the following anecdote: It is well known that there is a massive "control deficit" in data protection law in all EU member states. Recently, someone calculated that companies in Germany therefore only have to expect a review by the data protection authority every 200 years (!).