Introduction to the GDPR

I. Background

The EU Regulation 2016/79 "on the protection of natural persons with regard to the processing of personal data (GDPR) "[1] came into force on 25.5.2016 following publication in the official journal of the EU[2] on 4.5.2016 and started to apply as from 25.5.2018 (Art. 99).[3]

Until then the basis for a standardised form of data protection law in the EU was the EC Data Protection Directive of 24.10.1995.[4] A directive applies solely to Member States and is intended to harmonise regulated legal matter after being transposed into national law, which was accomplished inter alia by the BDSG. The harmonization effect relates particularly to the creation of equal economic conditions and equal terms of competition and can only be achieved if the national states keep within the margins assigned to them. This had not been sufficiently observed in practice.[5] This realization led to data protection in the EU now being organised in the form of a Regulation. Unlike Directives, Regulations have general and direct applicability and are in their entirety binding legal acts. Because of their direct applicability, they do not need to be transposed into national law by the Member States (Art. 288 Para. 2 TFEU).

On the other hand, a Regulation can have "escape clauses" which continue to allow regulations in national law or allow for national room for manoeuvre. In the GDPR this occurs in a number of cases. Some escape clauses give Member States a mandate for action; oth-

1. The full title is: "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)"
2. Official Journal L 119 of 4 May 2016; corrigendum: OJ EN 127/2 of 23 May 2018
3. In the following the Articles of the GDPR are listed without Regulation titles
4. Data Protection Directive 95/46/EG of 24.10.1995.
5. cf. CJEU of 24.11.2011 in the cases C-468/10 – ASNEF and C-469/10 – FECEMD; Lang, K&R 2012, 40

Einführung in die DS-GVO

I. Die Ausgangslage

Die EU-Verordnung 2016/79 „zum Schutz natürlicher Personen bei der der Verarbeitung personenbezogener Daten (DS-GVO)"[1] ist, nachdem sie am 4. 5. 2016 im Amtsblatt der EU[2] veröffentlicht wurde, am 25. 5. 2016 in Kraft getreten und hat seit dem 25. 5. 2018 (Art. 99) Geltung.[3]

Grundlage für die einheitliche Gestaltung des Datenschutzrechts in der EU war bis dahin noch die EG-Datenschutzrichtlinie vom 24.10.1995.[4] Eine Richtlinie ist mit dem Ziel der Harmonisierung der geregelten Rechtsmaterie ausschließlich an die Mitgliedstaaten gerichtet und von diesen in nationales Recht umzusetzen, was sodann u. a. im Bundesdatenschutzgesetz (BDSG) geschah. Der speziell unter dem Gesichtspunkt der Schaffung einheitlicher Wirtschaftsbedingungen und der Wettbewerbsgleichheit bedeutsame Harmonisierungseffekt wird aber nur erreicht, wenn die Nationalstaaten sich an die ihnen gewährten Spielräume halten. Dies war in der Praxis nicht hinreichend geschehen.[5] Auf Grund dieser Erkenntnis wird der Datenschutz in der EU nunmehr in einer Verordnung geregelt. Im Gegensatz zu Richtlinien sind Verordnungen allgemein und unmittelbar geltende und in allen ihren Teilen verbindliche Rechtsakte. Gemäß ihrer „Durchgriffswirkung" müssen sie von den EU-Mitgliedstaaten nicht in nationales Recht umgesetzt werden (Art. 288 Abs. 2 AEUV).

Andererseits kann eine Verordnung durch „Öffnungsklauseln" auch weiterhin Regulierungen im nationalen Recht gestatten bzw. nationale Gestaltungsspielräume eröffnen. Dies geschieht in der DS-GVO in gewichtiger Zahl. Einige Öffnungsklauseln geben den Mitglieds-

1. Der vollständige Titel lautet: „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April zum Schutz natürlicher Personenbei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)"
2. ABl. L 119 vom 4. Mai 2016, Berichtigung durch ABl. DE L 314/72 vom 22.11.2016 und ABl. DE L 127/2 vom 23.5.2018
3. Die Art. der DS-GVO werden nachfolgend ohne Verordnungstitel angegeben.
4. Datenschutzrichtlinie 95/46/EG vom 24.10.1995.
5. Vgl. EuGH vom 24.11.2011 in den Rechtssachen C-468/10 – ASNEF und C-469/10 – FECEMD; Lang, K&R 2012, 40

Entnommen aus: Müthlein (Hrsg.): Textausgabe DS-DVO deutsch-englisch ISBN 978-3-89577-837-1, 3. Auflage 2019

ers – and this is the majority – leave scope for action at the discretion of the Member States.[1] 50 to 60 saving clauses can be counted according to the method used. As a result the European data protection landscape continues to be complex and confusing.

II. The law on data protection under the GDPR

1. General

Building on the well-established principles of the EU Data Protection Directive, numerous topics are tackled which are also dealt with, for instance, in the key points of "modern data protection legislation" presented by the supervisory authorities.[2] This includes the revised formulation of the scope of protection, the technology-neutral approach, extended transparency obligations or special protection for minors. Other more recent calls for updating of data protection law are reflected in the regulation of "privacy by design and by default" (Art. 25), in data portability (Art. 20) and the special way in which erasure is organised in the form of the right to be forgotten (Art. 17 para. 2).

The principles for the processing of personal data laid out in Art. 5 of the Regulation form its main body. These include the principle of lawfulness, fairness and transparency, limitation to specific purposes, minimisation of data and storage, integrity and confidentiality and accountability.

It is not only the implementation of the principles embodied in these articles that entails time and effort in practical terms, but also the substantial amount of documentation work[3] falling on a company required to prove the fulfilment of its obligations.

1. cf. Veil, CR-online.de Blog of 1.2.2016-00.06;
2. Conference of the data protection commissioners of national and state governments: "Modern Data Protection Law for the 21st Century", resolution of 18 March 2010.
3. cf. Lepperhoff RDV 4/2016

staaten einen Handlungsauftrag; andere – und das ist die Mehrzahl – eröffnen einen in das Ermessen der Staaten gestellten Handlungsspielraum.[1] Je nach Zählweise kann man 50 bis 60 Öffnungsklauseln feststellen. Im Ergebnis stellt sich die europäische Datenschutzlandschaft auch weiterhin komplex und unübersichtlich dar.

II. Regelungen des Datenschutzes durch die DS-GVO

1. Allgemeines

Aufbauend auf den bewährten Prinzipien der EU-Datenschutzrichtlinie werden zahlreiche Themen angegangen, die auch z.B. Gegenstand der von den Aufsichtsbehörden[2] vorgelegten Eckpunkte eines „modernen Datenschutzrechts" sind. Dazu gehören die Neuformulierung der Schutzrichtung, der technikneutrale Ansatz, erweiterte Transparenzverpflichtungen oder der besondere Schutz Minderjähriger. Weitere aktuelle Forderungen der Fortschreibung des Datenschutzrechts finden ihren Niederschlag in der Regelung der „privacy by design and by default" (Art. 25), der Datenübertragbarkeit (Art. 20) und der speziellen Ausgestaltung der Löschung in Form des „Rechts auf Vergessenwerden" (Art. 17 Abs. 2).
Basis der Verordnung sind die in Art. 5 für die Verarbeitung personenbezogener Daten aufgestellten Grundsätze. Dazu gehören das Prinzip der Rechtmäßigkeit, der Richtigkeit, die Grundsätze von Treu und Glauben und der Transparenz, der Zweckbindung, der Daten- und Speicherminimierung, der Integrität und Vertraulichkeit und der Accountability.
Die Praxis belastet nicht nur die Umsetzung der die obigen Grundsätze konkretisierenden Artikel, sondern auch die umfangreichreichen Dokumentationsaufwendungen,[3] die das Unternehmen hinsichtlich des Nachweises seiner diesbezüglichen Verpflichtungen zu erfüllen hat.

1. Vgl. Veil, CR-online.de Blog vom 1.2.2016-00.06;
2. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: „Ein modernes Datenschutzrecht für das 21. Jahrhundert", Beschluss vom 18. März 2010
3. Vgl. hierzu im Einzelnen Lepperhoff, RDV 4/2016,

Entnommen aus: Müthlein (Hrsg.): Textausgabe DS-DVO deutsch-englisch ISBN 978-3-89577-837-1, 3. Auflage 2019

2. Scope of application

2.1 Material scope

According to Art. 2 para. 1, the Regulation applies to fully or partially automated processing of personal data and to the non-automated processing of personal data which are stored or are to be stored in a filing system.

2.1.1 Personal data

Personal data means any information on an identified or identifiable natural person, i.e. a "data subject" (Art. 4 (1). A person is identifiable when he or she can be identified either directly or indirectly by a controller or other person by means of reference to an identifier such as a name, identification number, location data, an online identifier or to one or more specific factors relating to the identity of that person. Data that can only be attributed to a natural person after the acquisition of additional information are deemed to be personal data if the controller or other person is generally considered to have the financial and technical means at their disposal to acquire this information. To this extent there is a difference between pseudonymised data and anonymous or anonymised information from which a data subject cannot or can no longer be identified.[1] There is no clear answer to the question of the relativity of the personal reference, i.e. whether data are regarded as pseudonymous for someone who has access to additional knowledge and anonymous for those to whom this does not apply.[2]

2.1.2 Processing

"Processing" refers to the handling of personal data, whether or not by automated means, that begins with collection and ends with erasure or destruction (Art. 4 (2)). Despite a considerably expanded catalogue of terms in Art. 4 relative to Art. 2 (b) of EU Directive 95/46/EC and the BDSG, the "classic" types of processing

1. cf. .See details in Recital 26
2. Cf. Gola, DS-GVO, Art. 4 Rdn. 16 ff. on the relativity of personal relatability

2. Geltungsbereich

2.1 Sachlicher Anwendungsbereich

Nach Art. 2 Abs. 1 findet die Verordnung Anwendung für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

2.1.1 Personenbezogene Daten

Mit einem personenbezogenem Datum wird jede Art von Informationen über eine bestimmte oder bestimmbare natürliche, d.h. „betroffene" Person gemeint (Art. 4 Nr. 1). Identifizierbar ist jemand, wenn er direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck seiner Identität sind, von dem Verantwortlichen oder einer anderen Person ermittelbar ist. Daten, die erst durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, gelten als personenbezogen, wenn dem Verantwortlichen oder anderen Personen zu deren Erlangung nach allgemeinem Ermessen finanzielle und technische Mittel zur Verfügung stehen. Insoweit unterscheiden sich pseudonymisierte Daten von anonymen bzw. anonymisierten Informationen, bei denen die betroffene Person nicht oder nicht mehr identifiziert werden kann.[1] Nicht eindeutig beantwortet bleibt die Frage nach der Relativität des Personenbezugs, d.h. ob Daten für den einen, der Zugang zu dem Zusatzwissen hat, als pseudonym und für andere, bei denen das nicht der Fall ist, als anonym gelten.[2]

2.1.2 Die Verarbeitung

Als „Verarbeitung" wird sodann jeder mit oder ohne Hilfe automatisierter Verfahren stattfindender Umgang mit personenbezogenen Daten, beginnend mit dem Erheben und endend mit dem Löschen oder Vernichten (Art. 4 Nr. 2), definiert. Trotz des in Art. 4 gegenüber Art. 2 Lit b EU-Rili 95/46/EG und dem

1. Vgl.im Einzelnen ErwG. 26
2. Zur Relativität des Personenbeziehbarkeit vgl. Gola, DS-GVO, Art. 4 Rdn. 16 ff.

Entnommen aus: Müthlein (Hrsg.): Textausgabe DS-DVO deutsch-englisch ISBN 978-3-89577-837-1, 3. Auflage 2019

such as those hitherto listed under Section 3 subsection 3-7 of the BDSG are no longer defined although, as in the case of transmission or erasure, they are regulated separately. One exception is "blocking" of data which now appears as the "right to restriction of processing" (Art. 4 (3)).

BDSG erheblich erweiterten Begriffskatalogs werden die bisherigen „klassischen" Erscheinungsformen der Verarbeitung z. B. des § 3 Abs. 3 bis 7 BDSG nicht mehr definiert, obwohl sie wie z. B. das Übermitteln oder das Löschen gesondert geregelt werden. Eine Ausnahme bildet das „Sperren" von Daten, das nunmehr als „Recht auf Einschränkung der Verarbeitung" firmiert (Art. 4 Nr. 3).

2.1.3 Automated/file-based procedure

This Regulation, too, only applies to a fully or partially automated processing of data or in cases when storage takes place in a filing system (Art. 2 para. 1) which is to be understood as manual processing as defined in Art. 4 (6) in a structured filing system. Oral questioning is also covered to the extent that the outcome is noted at least on file. The classic, unstructured file does not fall within the scope of the Regulation.

2.1.3 Automatisiertes/dateigebundenes Verfahren

Auch die Verordnung gilt „erst" bei einer ganz oder teilweise automatisierten Verarbeitung der Daten oder wenn ihre Speicherung in einem Dateisystem (Art. 2 Abs. 1) erfolgt, worunter eine in Art. 4 Nr. 6 definierte manuelle Verarbeitung in einem strukturierten Ablagesystem zu verstehen ist. Erfasst wird also auch die mündliche Befragung von Bewerbern, vorausgesetzt das Ergebnis wird zumindest dateimäßig notiert. Die klassische, unstrukturierte Akte fällt nicht unter die Verordnung.

2.2 Territorial scope

2.2.1 Controllers in the EU

The GDPR applies to any person who operates from an establishment within the Union, regardless of the location at which processing is conducted. The fact that a data subject has a job or habitual residence in a third country or is a foreign national is not relevant to his or her status as regards data protection (Recital 14).

2.2 Räumlicher Anwendungsbereich

2.2.1 In der EU ansässige Verantwortliche

Die DS-GVO zu beachten hat jeder, der – unabhängig von dem Ort, an dem die Verarbeitung erfolgt – von einer Niederlassung in der Union aus agiert (Art. 3 Abs. 1). Wenn der Betroffene seinen Arbeitsplatz bzw. Aufenthaltsort in einem Drittland hat oder ausländischer Staatsangehöriger ist, ändert das an seinen datenschutzrechtlichen Positionen nichts (ErwG. 14).

2.2.2 Controllers resident outside the EU

Processing on the part of a controller or processor not established or operating in the Union is covered by the Regulation provided the purpose of the data processing is related to services offered to data subjects in the EU or the monitoring of their behaviour (Art. 3 para. 2 lit. b). Like Art. 37 para. 1 lit.b regarding the obligation in this context to appoint a data protection officer[1], the norm targets the monitoring and evaluation of internet activities (Recital 24) and the compiling of client pro-

2.2.2 Außerhalb der EU ansässige Verantwortliche

Auch Verarbeitungen eines nicht in der Union Niedergelassenen bzw. von hieraus Agierenden werden u. a. erfasst, wenn die Datenverarbeitung dazu dient, das Verhalten von Personen in der EU zu beobachten oder ihnen Dienstleistungen anzubieten (Art. 3 Abs. 2 lit. b). Die Norm stellt – ebenso wie Art. 37 Abs. 1 lit. b hinsichtlich der diesbezüglichen Bestellpflicht eines Datenschutzbeauftragten[1] – ab auf die Beobachtung und Auswertung von Internetaktivitäten (ErwG. 24) und die

1. Weichert, CuA 4/2016, 9

1. Weichert, CuA 4/2016, 9

files. There is nevertheless no apparent reason why it should not be applicable in the case of employee data processing. An ongoing performance and conduct data evaluation and the human resources system assessing employee conduct of an international enterprise established in a third country also meet the statutory definition.[1]

3. Norm addressees

3.1 The data processing controller

The norm addressee, the person called the controller (Art. 4 (7))[2] is the natural or legal person, authority, agency or other body who either alone or with others decides on the purpose and means of processing, whereby in bodies such as a corporate association several controllers can cooperate with one another (Art. 26).

3.2 The processor

Direct responsibilities are henceforth allocated to bodies described as processors, these being agencies that process personal data as directed by the controller (Art. 3 (8)). The processor does not become a "third party" if his establishment is in a third country (Art. 4 (10)). Adherence by the processor to the obligation to apply the required technical and organisational measures can now be demonstrated (Art. 28 para. 5) by means of codes of conduct pursuant to Art. 40 (code of conduct) or certification pursuant to Art. 42. If a processor ignores instructions regarding adherence to the purpose and means of processing, the processor shall be held responsible as the controller for this unauthorised processing (Art. 28 para. 10).[3] The processor, together with a controller where applicable, can be held liable for any material or immaterial damage resulting from unlawful data processing (Art. 82 para. 1).

1. So Wybitul/Fladung, BB 2012, 509
2. cf. Monreal, ZD 2014, 611 on terminology
3. cf. Petri, ZD 2015, 305; Müthlein, RDV 2016, 74 on commissioned data processing in the GDPR

Erstellung von Kundenprofilen. Gleichwohl ist nicht erkennbar, weshalb sie bei Beschäftigtendatenverarbeitung nicht anwendbar sein sollte. Eine dauernde Auswertung von Leistungs- und Verhaltensdaten und ein das Mitarbeiterverhalten bewertendes Human Resource-System eines im Drittland ansässigen internationalen Konzerns erfüllt den Tatbestand daher ebenfalls.[1]

3. Normadressaten

3.1 Der Datenschutz „ Verantwortliche"

Normadressat, der als der „ Verantwortliche" bezeichnet wird (Art. 4 Nr. 7),[2] ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, wobei z.B. innerhalb eines Unternehmensverbunds auch mehrere als gemeinsam Verantwortliche kooperieren können (Art. 26).

3.2 Auftragsverarbeiter

Unmittelbar mit Pflichten belegt werden auch nunmehr als „Auftragsverarbeiter" bezeichnete Stellen, d.h. Stellen, die personenbezogene Daten weisungsgebunden für den Verantwortlichen verarbeiten (Art. 3 Nr. 8). Der Auftragnehmer wird nicht zum „Dritten", wenn er seinen Sitz im Drittland hat (Art. 4 Nr. 10). Die Einhaltung der Pflichten des Auftragnehmers zur Einhaltung der erforderlichen technisch- organisatorischen Maßnahmen kann durch Anwendung von Verhaltensregelungen nach Art. 40 (code of conduct) oder eine Zertififizierung nach Art. 42 nachgewiesen werden (Art. 28 Abs. 5). Setzt sich der Auftragnehmer über die ihm gegebenen Weisungen hinsichtlich der Bindung an die Zwecke und Mittel der Datenverarbeitung hinweg, ist er für diese unautorisierte Verarbeitung als Verantwortlicher in Rechenschaft zu ziehen (Art. 28 Abs. 10).[3] Der Auftragsverarbeiter hat ggf. gemeinsam mit seinem Auftraggeber für einen bei ihnen infolge rechtswidriger Datenverarbeitung eingetretenen materiellen und immateriellen Schaden zu haften (Art. 82 Abs. 1).

1. So Wybitul/Fladung, BB 2012, 509
2. Zum Begriff vgl. bei Monreal, ZD 2014, 611
3. Vgl. zur AuftragsDV nach der DS DS-GVO im einzelnen bei Petri, ZD 2015, 305; Müthlein, RDV 2016, 74

Entnommen aus: Müthlein (Hrsg.): Textausgabe DS-DVO deutsch-englisch ISBN 978-3-89577-837-1, 3. Auflage 2019

3.3 Data processing employees/data confidentiality

Art. 29 of the GDPR addresses persons with access to personal data responsible to the controller or processor and to processors themselves and specifies that as a general principle they should only process personal data on instruction from the controller responsible for processing. An obligation by private employers to commit employees to confidentiality on commencement of their duties only exists in indirect form; processors are obliged to ascertain whether persons authorized by them to process personal data have undertaken to observe confidentiality or whether they are covered by an appropriate statutory confidentiality obligation (Art. 28 para. 3 lit. b).

3.4 Data protection officer

The data protection officer introduced in all Member States is also allocated statutory responsibilities (Art. 37ff). However, the GDPR only stipulates an obligation to designate to those private bodies whose core activity involves carrying out processing that requires regular and systematic monitoring of data subjects on a large scale or which involves processing special categories of data pursuant to Article 9 para. 1 or of data on criminal convictions and offences as in Art. 9. The question as to when monitoring of employees meets the statutory definition[1] can be irrelevant for German employers as German legislation, in the light of the escape clause in Art. 37 para. 4 sentence 1, retains in Section 38 of the BDSG the previous provisions relating to the obligation to designate. The responsibilities of the data protection officer now include increasing compliance and monitoring functions which leads to the question of his guarantor function in the penal and administrative offence context.[2]

1. Cf. preceding section 3.2 and Weichert CuA 4/2016, 4
2. cf. Wybitul, ZD 2016, 203

3.3 Die bei der Datenverarbeitung Beschäftigten/Datengeheimnis

Die DS-GVO wendet sich in Art. 29 auch an Personen, die dem Verantwortlichen oder seinen Auftragsverarbeitern unterstellt sind und Zugang zu personenbezogenen Daten haben, und auch an den Auftragsverarbeiter selbst und gibt ihnen vor, personenbezogene Daten grundsätzlich nur auf Anweisung des für die Verarbeitung Verantwortlichen zu verarbeiten. Eine Pflicht privater Arbeitgeber, die Beschäftigten bei Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten, besteht indirekt, indem Auftragsverarbeiter sicherzustellen haben, dass die von ihnen zur Verarbeitung personenbezogener Daten autorisierten Personen sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b).

3.4 Datenschutzbeauftragter

Gesetzliche Pflichten werden auch dem für alle Mitgliedstaaten eingeführten Datenschutzbeauftragten zugewiesen (Art. 37 ff). Die DS-GVO sieht eine Bestellpflicht jedoch nur für solche privaten Stellen vor, deren Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche eine regelmäßige und systematische Beobachtung von betroffenen Personen im großem Umfang erforderlich machen oder die Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 Abs. 1 im großem Umfang oder von Daten zu strafrechtlichen Verurteilungen und Straftaten im Sinne des Art. 9 zum Gegenstand haben. Die Frage, ab wann eine Überwachung von Beschäftigten den Tatbestand erfüllt,[1] kann für deutsche Arbeitgeber dahinstehen, da der deutsche Gesetzgeber gemäß der Öffnungsklausel in Art. 37 Abs. 4 S. 1 für die Bestellpflicht an den bislang geltenden Bestimmungen im § 38 BDSG festgehalten hat. Die Aufgabenstellung des Datenschutzbeauftragten hat nunmehr verstärkt Compliance- und Überwachungsfunktionen, woraus sich die Frage nach seiner Garantenfunktion im straf- und ordnungswidrigkeitrechtlichen Sinne ergibt.[2]

1. Vgl. vorstehen Abschnitt 3.2 und Weichert CuA 4/2016, 4
2. Vgl. Wybitul, ZD 2016, 203

Entnommen aus: Müthlein (Hrsg.): Textausgabe DS-DVO deutsch-englisch ISBN 978-3-89577-837-1, 3. Auflage 2019

Introduction to the GDPR

3.5 The supervisory authority

Broad scale regulations on the competence and in particular cooperation between the supervisory authorities of Member States are intended to bring about a EU-wide uniform supervisory system[1] and efficient application of the law by data protection authorities in the single market. A European Data Protection Board equipped with extensive authorities (Art. 68 ff) consisting of representatives of the national supervisory authorities is charged with maintaining uniform application of data protection law. Parallel to this a so-called "one stop shop" approach[2] is designed to make it easier for data subjects and responsible enterprises to interact with data protection supervisors in creating central public authority responsibility. It also gives an assurance that data subjects can always approach the authority responsible for their place of residence or employment (Art.77). Where there are several responsible bodies, a so-called consistency mechanism safeguards uniform application of the Regulation. The GDPR provides for severe penalties in an effort to underline the importance of practical implementation of the data protection regulations. Fines are increased drastically. Enterprises can be faced with fines of up to 20 million euros or – for instance in the case of infringement of basic principles such as in compliances, the rights of data subjects or the rules for international data transmission – fines for affiliates of up to four percent of their global annual turnover. The broad statutory definitions of a fine offence leave hardly any non-observance of the GDPR regulations without sanction.

4. Admissibility of processing

4.1 Ban subject to the possibility of authorisation

A basic principle of the GDPR is that the processing of personal data is governed by a ban subject to authorisation[3], meaning that any form of processing is only admissible with the consent of the data subject or if the

1. See Lüdemann/Wenzel, RDV 2015, 285 on the current situation in Germany and the GDPR.
2. Nguyen, ZD 2015, 265

Einführung in die DS-GVO

3.5 Die Aufsichtsbehörden

Umfangreiche Regelungen zur Kompetenz und insbesondere zur Zusammenarbeit der Aufsichtsbehörden der Mitgliedstaaten sollen eine EU-weite einheitlichere Aufsichtspraxis[1] und effektive Rechtsdurchsetzung der Datenschutzbehörden im Binnenmarkt bewirken. Ein mit weitreichenden Kompetenzen ausgestatteter Europäischer Datenschutzausschuss (Art. 68 ff), bestehend aus Vertretern der nationalen Aufsichtsbehörden, soll die einheitliche Anwendung des Datenschutzrechts sicherstellen. Parallel dazu soll der sog. „One-Stop-Shop"-Ansatz[2] Betroffenen und verantwortlichen Unternehmen die Interaktion mit der Datenschutzaufsicht erleichtern, indem eine zentrale Behördenzuständigkeit begründet wird. Gleichzeitig wird damit gewährleistet, dass sich der Betroffene immer an die für seinen Wohnsitz oder Arbeitsplatz zuständige Behörde wenden kann (Art. 77). Bei mehreren Zuständigkeiten wird im sog. Kohärenzverfahren eine einheitliche Anwendung der Verordnung sichergestellt. Um der Notwendigkeit einer praktischen Umsetzung der Datenschutzvorschriften Nachdruck zu verleihen, sieht die DS-GVO empfindliche Sanktionen vor. Gegenüber Unternehmen können Bußgelder bis zu 20 Mio Euro oder z. B. bei einer Verletzung von wesentlichen Grundprinzipien, bspw. in Bezug auf Einwilligungen, Betroffenenrechte oder die Regeln für die internationale Datenübermittlung, Geldbußen bei Konzerngesellschaften bis zu vier Prozent des weltweiten Jahresumsatzes verhängt werden. Die umfangreichen Bußgeldtatbestände lassen kaum eine Missachtung von Vorschriften der DS-GVO sanktionsfrei (siehe Art.83 Abs. 2).

4. Zulässigkeit der Verarbeitung

4.1 Verbot mit Erlaubnisvorbehalt

Grundprinzip der DS-GVO ist, dass die Verarbeitung personenbezogener Daten unter einem Verbot mit Erlaubnisvorbehalt steht,[3] d. h. jede Form der Verarbeitung ist nur zulässig, wenn der Betroffene eingewilligt

1. Zur aktuellen Situation in Deutschland und der DS-GVO Lüdemann/Wenzel, RDV 2015. 285
2. Hierzu Nguyen, ZD 2015, 265

Entnommen aus: Müthlein (Hrsg.): Textausgabe DS-DVO deutsch-englisch ISBN 978-3-89577-837-1, 3. Auflage 2019

Regulation itself has given its consent. Articles 6 and 7 describe the norms allowing data processors to process data without the consent or even contrary to the will of employees.

4.2 Consent

Article 6 para. 1 lit.a lists consent as the first statutory criteria for permissibility. Art. 4 (11) states that it must be given freely. Recital 43 states in general terms that consent is no legal basis for data processing if there is a clear imbalance between the data subject and the controller responsible for processing. It is not assumed, as a Commission proposal[1] initially envisaged, that there is an imbalance in an employment relationship that generally excludes consent.[2] Recital 42 sentence 5 also states that it can only be assumed that the consent of an employee is freely given if he or she has a genuine or free choice and is thus in a position to refuse or withdraw consent without suffering any disadvantage. On the other hand the Recital allows requiring consent as a "conditio sine qua non" if consent is necessary for the fulfilment of a contract.

A specific, informed statement is required (Art. 4 (11)) meaning that blanket or global consent for the processing of personal data is not valid.

Art. 7 para. 3 states that consent can be withdrawn at any time. This is in line with previous law. The Regulation does not apparently regard it as an abuse of the law if employees are deceived about their alleged right to self-determination when giving what turns out to be irrelevant consent as the Regulation permits the con-

3. cf.Horning ZD2012, 101 on this concept which has rightly been described as "welcome".
1. COM/2012/011 final; Gola, EuZW 2012, 332
2. cf. Also the Federal Labour Court on the admissibility of images published in the internet based on consent given by employees, RDV 2015, 259; also the parallel decision, ZD 2015, 380 with comment Tiedemann

hat oder die Verordnung selbst die Einwilligung erteilt. Die Erlaubnisnormen der Verordnung, die dem Datenverarbeiter Datenverarbeitungen auch ohne oder sogar gegen den Willen des Beschäftigten gestatten, geben die Art. 6 und 7 wieder.

4.2 Die Einwilligung

Artikel 6 Abs. 1 lit. a nennt die Einwilligung an erster Stelle als Erlaubnistatbestand. Gemäß Art. 4 Nr. 11 muss sie freiwillig („freely given") erteilt werden. In ErwG. 43 wird dazu allgemein ausgeführt, dass eine Einwilligung dann keine Rechtsgrundlage für die Datenverarbeitung darstellt, wenn ein klares Ungleichgewicht zwischen dem Betroffenen und dem für die Verarbeitung Verantwortlichen besteht. Nicht unterstellt wird, wie ein erster Kommissionsvorschlag[1] es noch vorsah, dass im Arbeitsverhältnis ein solches Einwilligungen generell ausschließendes Ungleichgewicht bestehe.[2] Nach ErwG. 42 S. 5 sollte auch nur dann davon ausgegangen werden, dass der Beschäftigte die Einwilligung freiwillig abgibt, wenn er eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Andererseits lässt aber ErwG. 43 S. 2 die Einholung der Einwilligung als „conditio sine qua non" zu, wenn die Einwilligung für die Erfüllung eines Vertrages erforderlich ist.
Verlangt wird eine konkrete, informierte Erklärung (Art. 4 Nr. 11), so dass pauschale oder globale Einwilligungen für den Umgang mit personenbezogenen Daten nicht wirksam sind.
Nach Art. 7 Abs. 3 kann die Einwilligung jederzeit widerrufen werden. Dies entspricht bereits der geltenden Rechtslage. Nicht als rechtsmissbräuchlich sieht es die Verordnung offensichtlich an, wenn der Beschäftigte bei Einholung einer im Endeffekt belanglosen Einwilligung über sein vermeintliches Selbstbestimmungsrecht getäuscht wird, weil die Verordnung

3. Vgl. zu dieser zu Recht als „begrüßenswert" bezeichneten Konzeption Hornung ZD 2012, 101
1. KOM/2012/011 endgültig; Gola, EuZW 2012, 332
2. Vgl. insoweit auch BAG zur Zulässigkeit von Bildveröffentlichungen im Internet auf Grund erteilter Einwilligung der Beschäftigten, RDV 2015, 259; ferner die Parallelentscheidung, ZD 2015, 380 mit Anm. Tiedemann

troller to refer to another norm permitting processing despite consent being withdrawn.

4.3 Assigned purpose resulting from a contractual relationship

The Regulation then permits processing for purposes linked to a contract with the data subject or a pre-contractual relationship (Art. 6 para. 1 lit. b). This means that a – potential – contract partner is allowed to process data when they are required for the justification, implementation or ending of a prospective contractual relationship.

4.4 Balance of interests

If data are involved that are not part of contractual relationships, the balance of interests clause of Art. 6 para. 1 lit. f may be referred to. This states that the lawfulness of processing can be justified by the legitimate interests of the controller or a third party. In the event of appropriate balancing of interests, consideration must be given to the reasonable expectations of the data subject which can include considerations such as being an employee or customer of the controller (Recital 47 sentence 2).

Recital 48 states that controllers who are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting the personal data of employees within the group for internal administrative purposes. According to Art. 4 (19) and Recital 37, a "group of undertakings" means a controlling undertaking and the undertakings it controls. A central undertaking that controls the processing of personal data in affiliated undertakings forms a unit with these which can also be treated as a group of undertakings. Hence the GDPR contains no privilege for multicorporate enterprises but does make clear that special multicorporate interests can have special significance in balancing the interests worthy of protection of employees in the context of Art. 6 para. 2 lit. f or also in drawing up company agreements.

dem Verantwortlichen erlaubt, sich nunmehr trotz Widerruf ggf. auf eine andere Erlaubnisnorm für die Verarbeitung zu berufen.

4.3 Sich aus einer vertraglichen Beziehung ergebende Zweckbestimmung

Die Verordnung gibt die Erlaubnis sodann für Zwecke, die sich aus einem mit dem Betroffenen abgeschlossenen Vertrag bzw. einer vorvertraglichen Beziehung ergeben (Art. 6 Abs. 1 lit. b), d. h. ein – potentieller – Vertragspartner darf die Daten verarbeiten, die erforderlich sind für die Begründung, Durchführung und Beendigung der in Betracht kommenden vertraglichen Beziehung.

4.4 Die Interessenabwägung

Handelt es sich um außerhalb vertraglicher Beziehungen benötigte Daten, kann auf die Interessenabwägungsklausel des Art. 6 Abs. 1 lit. f zurückgegriffen werden. Danach kann die Rechtmäßigkeit der Verarbeitung durch die berechtigten Interessen des Verantwortlichen oder auch eines Dritten begründet sein. Bei der gebotenen Interessenabwägung sind die vernünftigen Erwartungen der betroffenen Person zu berücksichtigen, die sich u. a. daraus ergeben können, dass sie in den Diensten des Verantwortlichen steht oder dessen Kunde ist (ErwG. 47 S. 2).
Nach ErwG. 48 sollen Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, ggf. ein berechtigtes Interesse haben, personenbezogene Daten von Mitarbeitern innerhalb der Unternehmensgruppe für interne Verwaltungszwecke zu übermitteln. Gemäß Art. 4 Nr. 19 und ErwG. 37 versteht man unter einer „Unternehmensgruppe" ein herrschendes und von diesem abhängige Unternehmen. Ein zentrales Unternehmen, das die Verarbeitung personenbezogener Daten in angeschlossenen Unternehmen kontrolliert, bildet mit diesen eine Einheit, die ebenfalls als Unternehmensgruppe behandelt werden kann. Die DS-GVO enthält damit zwar kein Konzernprivileg, macht aber doch deutlich, dass spezielle Konzerninteressen in der Abwägung mit den schutzwürdigen Interessen der Beschäftigten im Rahmen des Art. 6 Abs. 2 lit. f oder auch bei der Gestaltung von Betriebsvereinbarungen ein besonderes Gewicht haben können.

Entnommen aus: Müthlein (Hrsg.): Textausgabe DS-DVO deutsch-englisch ISBN 978-3-89577-837-1, 3. Auflage 2019

Introduction to the GDPR

4.5 Compliance with statutory provisions

Processing is automatically permissible if it is required for complying with a legal obligation resulting from EU law or from the law of Member States that satisfies data protection principles (Art. 2 lt.c) or when processing is necessary in order to be able to carry out a function in the public interest or in the execution of sovereign powers assigned to the controller for the processing (Art. 6 para. 2 lit.e). This means that, for instance, the processing of data in a payroll programme required on the grounds of legal stipulations is fully justifiable.

4.6 Sensitive data

Special regulations (Art. 9 para. 2) overriding Art. 6 GDPR apply to the specific categories of personal data named in Art. 9 para. 1. Members of a trade union and the genetic and biometric data used for the unique identification of a person as defined in Art. 4(13) and (14) are added to those already mentioned in Art. 8 (1) of EU Diretive 95/46/EC and Section 3 para. 9 BDSG (old version).

Worth noting here is that the legal conditions for consent in Art. 9 para. 2 are stricter than in Art. 6. On the other hand, Art. 9 para. 2 lit. b explicitly permits processing that is necessary in order for an employer or employee to comply with rights and obligations arising from labour law and social security and social protection law.

Finally, Art. 9 para. 4 includes an escape clause whereby Member States can introduce further provisions including limitations in the processing of genetic, biometric and health data.

4.7 Criminal convictions and offences

Art. 10 stipulates that data on criminal convictions and offences may only be processed where this is permissible under the law of a Member State with adequate guarantees for the rights of the data subjects. It must be assumed that a concrete area-specific provision is

Einführung in die DS-GVO

4.5 Erfüllung gesetzlicher Vorgaben

Eine Verarbeitung ist zwangsläufig auch dann gestattet, wenn sie für die Erfüllung einer rechtlichen Verpflichtung erforderlich ist, die sich aus dem EU-Recht oder Datenschutzgrundsätzen genügendem Recht eines Mitgliedstaats ergibt (Art. 6 Abs. 2 lit. c) oder wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung von dem für die Verarbeitung Verantwortlichen übertragener hoheitlicher Gewalt erfolgt (Art. 6 Abs. 2 lit. e). Damit ist z. B. die Zulässigkeit der Verarbeitung der auf Grund gesetzlicher Vorgaben in einem Gehaltsabrechnungsprogramm erforderlichen Daten durchweg gerechtfertigt.

4.6 Sensible Daten

Besondere, dem Art. 6 DS-GVO vorrangige Zulässigkeitsregelungen (Art. 9 Abs. 2) gelten für die in Art. 9 Abs.1 benannten besonderen Kategorien personenbezogener Daten. Ergänzend zu den bereits in Art. 8 Abs. 1 EU-Rili 95/46/EG bzw. § 3 Abs. 9 BDSG a. F. genannten zählen hierzu die Gewerkschaftszugehörigkeit und der eindeutigen Identifizierung einer Person dienende genetische und biometrische Daten, die in Art. 4 Nr. 13 und 14 definiert werden.
Die eigentliche Besonderheit liegt darin, dass die Erlaubnistatbestände des Art. 9 Abs. 2 strengere Voraussetzungen beinhalten als Art. 6. Andererseits erlaubt Art. 9 Abs. 2 lit. b ausdrücklich die Verarbeitung, wenn sie erforderlich ist, damit der Arbeitgeber oder der Beschäftigte den ihm aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte bzw. Pflichten nachkommen bzw. erhalten kann.
Schließlich enthält Art. 9 Abs. 4 eine Öffnungsklausel, nach der die Mitgliedstaaten weitere Bestimmungen, einschließlich Beschränkungen, zur Verarbeitung genetischer, biometrischer und Gesundheitsdaten beibehalten oder einführen können.

4.7 Strafurteile und Straftaten

Nach Art. 10 darf die Verarbeitung von Daten über Strafurteile und Straftaten nur erfolgen, wenn diese nach dem Recht des Mitgliedstaates unter angemessenen Garantien für die Rechte der betroffenen Person zulässig ist. Auszugehen ist davon, dass eine konkrete be-

Entnommen aus: Müthlein (Hrsg.): Textausgabe DS-DVO deutsch-englisch ISBN 978-3-89577-837-1, 3. Auflage 2019