Vermerk: Abdingbarkeit von TOMs (Art. 32 DSGVO)

1. Fragestellung und grundsätzliche Erwägungen

Art. 32 DSGVO sieht vor, dass Verantwortliche und Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um die Rechte und Freiheiten der betroffenen Personen zu schützen. Die Sicherheit der Verarbeitung ist durch den Verantwortlichen oder den Auftragsverarbeiter durch Pseudonymisierung oder Verschlüsselung der personenbezogenen Daten sowie durch die Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme sicherzustellen. Die DSGVO schreibt dabei in Art. 32 DSGVO kein bestimmtes Schutzniveau vor, sondern verpflichtet den Verantwortlichen zu einer Abwägung zwischen den Risiken der Verarbeitung und den Implementierungskosten sowie der Art, dem Umfang, der Umstände und dem Zweck der Verarbeitung.

Aus Erwägungsgrund 83 DSGVO ergibt sich, nach welchen Maßstäben diese Abwägung zu erfolgen hat:

„Bei der Bewertung der Datensicherheitsrisiken sollten die mit der Verarbeitung personenbezogener Daten verbundenen Risiken berücksichtigt werden, wie etwa – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnte.“

Als Zweck der Regelung gibt Erwägungsgrund 83 DSGVO an:

„Diese Maßnahmen sollten unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau (…) gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist.“

Der Verantwortliche oder der Auftragsverarbeiter hat mithin zu prüfen, welche Risiken sich aus den genannten Szenarien ergeben können. Diese hat er ins Verhältnis zu den Kosten möglicher Schutzmaßnahmen zu setzen. Ausgangspunkt ist bei alledem der Stand der Technik (Art. 32 Abs. 1 DSGVO). Welche Maßnahmen konkret erforderlich sind, kann er in Anlehnung an anerkannte Sicherheitsmaßnahmenkataloge wie dem BSI-Grundschutz, der ISO 27001 oder dem Standard-Datenschutzmodell prüfen.[1] Im Ergebnis verbleibt ihm bei der Festlegung der Schutzmaßnahmen

[1] Mantz, in: Sydow, DSGVO, 2. Aufl. 2018, Art. 32 DSGVO Rn. 36.

dabei ein (Beurteilungs-)Spielraum.[2] Dieser entfällt, wenn der Verantwortliche zu einer ganz bestimmten Schutzmaßnahme von Rechts wegen verpflichtet ist. Dies dürfte die Ausnahme bleiben,[3] da es insoweit auf eine Gesamteinschätzung der ergriffenen Schutzmaßnahmen ankommt, die den erforderlichen Schutz erst in ihrer Gesamtheit gewährleisten müssen.[4] Allerdings kann der Schutzbedarf der Daten es erfordern, dass zumindest eine von mehreren denkbaren technischen Schutzmaßnahmen ergriffen wird, wenn dies dem Stand der Technik entspricht.

In Wissenschaft und Praxis wird diskutiert, ob betroffene Personen in ein niedrigeres Schutzniveau einwilligen können als rechtlich geboten ist. Die Problematik zeigt sich in der Praxis typischerweise anhand der (E-Mail-)Verschlüsselung. In den problematischen Fällen ergibt die Abwägung nach Art. 32 DSGVO, dass eine Ende-zu-Ende-Verschlüsselung geboten ist, da es sich beispielweise um besonders schutzwürdige personenbezogene Daten nach Art. 9 DSGVO handelt. Verfügen allerdings entweder der Verantwortliche oder die betroffene Person nicht über die entsprechenden technischen Mittel um eine solche Verschlüsselung umzusetzen, stellt sich die Frage,[5] ob und unter welchen Voraussetzungen die betroffene Person in ein niedrigeres Schutzniveau einwilligen kann. Es geht also um die Frage, ob oder inwieweit es sich bei den Vorgaben des Art. 32 DSGVO um zwingende, nicht zur Disposition der betroffenen Person stehende Vorgaben handelt.

[2] Jandt, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, Art. 32 DSGVO Rn. 8; Mantz, in: Sydow, DSGVO, 2. Aufl. 2018, Art. 32 DSGVO Rn. 10.
[3] Ebenso Piltz, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 32 DSGVO Rn. 3.
[4] Jandt, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, Art. 32 DSGVO Rn. 5; Martini, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DSGVO Rn. 26.
[5] Die technische Umsetzbarkeit kann auch an der Kompatibilität der eingesetzten Systeme scheitern: Schöttle/Ludwig, BRAK-Mitteilungen 2020, 312, 313.

2. Ist Systemdatenschutz zwingendes, unabdingbares Recht?

Die Frage, ob Art. 32 DSGVO zwingendes, nicht zur Disposition stehendes Recht darstellt,[6] wird teilweise mit dem Argument bejaht, dass die DSGVO einen europäischen Mindeststandard des Systemdatenschutzes schaffen wolle. Damit sich ein solcher europaweit einheitlich etablieren könne, sei es erforderlich, dass die Vorgaben des Art. 32 DSGVO auch umgesetzt werden und nicht durch Vereinbarungen mit den betroffenen Personen unterlaufen werden können. Hintergrund dieser Argumentation ist die Befürchtung, dass der Systemdatenschutz ansonsten aufgrund wirtschaftlicher Erwägungen der Verantwortlichen auf ein minimales Niveau reduziert würde.[7] Eine Plattform mit vielen Nutzern könnte anstatt einer kostspieligen Anpassung ihrer Systeme an den Stand der Technik einfach eine Vereinbarung mit sämtlichen Nutzern darüber treffen, dass diese in die Nutzung der Plattform trotz der Risiken der veralteten Technik einwilligen. Gerade bei Anbietern, deren Kunden keine vergleichbaren Alternativen haben oder bei denen die Nutzer ihr Netzwerk auf der Plattform aufgebaut haben („lock-in-Effekt“), dürfte es leicht fallen, entsprechende Erklärungen der Nutzer einzuholen. Dies würde dem Ziel der DSGVO zuwiderlaufen, den Datenschutz durch Technikgestaltung (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) zu fördern (vgl. Art. 25 Abs. 1 und ErwGr. 78 Satz 2 DSGVO).

Diese Erwägungen sind berechtigt. Gleichzeitig würde es jedoch eine erhebliche Beschränkung der Entscheidungsfreiheit der betroffenen Personen bedeuten, wenn eine Verarbeitung ihrer personenbezogenen Daten, die sie ausdrücklich wünschen, mit Verweis auf den Systemdatenschutz nicht durchgeführt werden kann. Dies ist bei Arztpraxen, Steuerberatern oder Anwälten zu beobachten, die Auskünfte oder die Übermittlung dringend benötigter Unterlagen per einfacher E-Mail nicht durchführen, da sie befürchten Art. 32 DSGVO zuwiderzuhandeln, selbst wenn die betroffene Person ausdrücklich in die unsichere Übermittlungsart einwilligt. Es dürfte weder

[6] Gegen die Abdingbarkeit: Jandt, in Kühling/Buchner, DS-GVO, 3. Aufl. 2020, Art. 32 DSGVO Rn. 40, die nur bei der Wahl der Mittel eine Wahlmöglichkeit für zulässig erachtet; Zur alten Rechtslage auch noch HmbBfDI, Tätigkeitsbericht Datenschutz 2018, S. 122 und HmbBfDI, Schreiben vom 8.1.18, S. 2, abrufbar unter https://www.dr-datenschutz.de/wp-content/uploads/2018/02/schreiben-der-aufsichtsbehoerde.pdf;
Für eine Abdingbarkeit: Römermann/Praß, in: BeckOK BORA, 30. Edition 2020, § 2 BORA Rn. 43 -44; Wagner, BRAK-Mitteilungen 4/2019, 167, 171 zitiert nach VG Mainz Urt. v. 17.12.2020 – 1 K 778/19.MZ, BeckRS 2020, 41220, Rn. 42, das die Frage offen lässt; VG Berlin Urt. v. 24.5.2011 – Az. 1 K 133/10, BeckRS 2011, 52814; Bay. Landesamt für Datenschutzaufsicht, Tätigkeitsbericht 2015/16, S. 99; Zusammenfassung des Streitstandes bei Martini, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DSGVO Rn. 4a-4d.
[7] Hornung, ZD 2011, 51, 52.

im Sinne des Verordnungsgebers noch der betroffenen Person sein, dieser gegen ihren Willen und möglicherweise zu ihrem Nachteil ein Schutzniveau aufzuzwingen, das sie ausdrücklich ablehnt.[8]

Aufgrund dieser widerstreitenden Interessen ist die Frage der Abdingbarkeit des Systemdatenschutzes daher nicht pauschal zu beantworten. Die Antwort muss insbesondere zwischen dem Verantwortlichen oder Auftragsverarbeiter und der betroffenen Person differenzieren.

a. Unterscheidung zwischen betroffener Person und Verantwortlichem

Art. 32 DSGVO enthält Pflichten für den Verantwortlichen oder Auftragsverarbeiter, die zwar einen Beurteilungsspielraum zulassen, im Kern allerdings zwingend sind und nicht zur Disposition des Verantwortlichen oder Auftragsverarbeiters stehen. Etwas anderes gilt in Bezug auf die betroffene Person, da die DSGVO ausweislich des Art. 1 Abs. 2 DSGVO „die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“ zu ihrem Regelungsgegenstand erklärt. Primäres Schutzgut ist also das Grundrecht auf Datenschutz (Art. 8 GRCh). Dieses steht zur Disposition des Grundrechtsträgers, also der betroffenen Person. Dies zeigt sich bereits auf grundrechtlicher Ebene, da schon Art. 8 Abs. 2 Satz 1 GRCh zentral auf die Einwilligung der betroffenen Person abhebt. Es ist der betroffenen Person grundsätzlich unbenommen, in alle möglichen Formen von Verarbeitungen ihrer personenbezogenen Daten einzuwilligen, auch wenn diese möglicherweise von Außenstehenden als für die betroffene Person schädlich wahrgenommen werden. So kann darin eingewilligt werden, dass unvorteilhafte oder sexualisierte Aufnahmen im Internet veröffentlicht werden. Auch könnte die betroffene Person darin einwilligen, dass die Zugangsdaten zu ihrem Bankkonto oder ihre Gesundheitsdaten veröffentlicht werden. Ob dies in ihrem Sinne oder im Sinne des Datenschutzes ist, spielt dabei keine Rolle, solange eine wirksame Einwilligung vorliegt. Es erscheint vor diesem Hintergrund nicht überzeugend, anzunehmen, dass zwar eine Einwilligung in die direkte Veröffentlichung von personenbezogenen Daten möglich sei, nicht aber das Übermitteln solcher Daten auf einem Weg, der nicht ausreichend gesichert ist. Die schlimmste Folge wäre ein Ausspähen und eine nicht mehr kontrollierbare allgemeine Veröffentlichung. In diese könnte die betroffene Person aber ohnehin einwilligen.

[8] Zu § 9 BDSG a.F.: VG Berlin, Urt. v. 24.05.2011 - 1 K 133.10, Rn. 24.

Vermerk: Abdingbarkeit von TOMs (Art. 32 DSGVO)

Die Vorgaben der europäischen Grundrechte, welche die DSGVO nach Art. 1 Abs. 2 DSGVO umsetzt, sprechen also dafür, dass die Schutzmaßnahmen bei der Verarbeitung der eigenen personenbezogenen Daten durch die betroffene Person abdingbar sind. Dies umfasst auch die technischen Mittel, die zu der Verarbeitung eingesetzt werden (oder eben nicht eingesetzt werden).[9]

Art. 32 DSGVO stützt diese Schlussfolgerung, da sich aus seinem Wortlaut zwei Ziele ableiten lassen: Primär der Schutz der betroffenen Person[10] und sekundär die Etablierung eines hohen, europaweit einheitlichen Niveaus der Datensicherheit. So bezieht sich Art. 32 Abs. 1 DSGVO explizit auf das „Risiko[…] für die Rechte und Freiheiten natürlicher Personen". Art. 32 DSGVO verfolgt daneben - wie die gesamte DSGVO[11] - noch das Regelungsziel, ein einheitliches Niveau der Datensicherheit bei der Verarbeitung personenbezogener Daten zu schaffen. Das sekundäre Ziel wird auch dann erreicht, wenn ein Verzicht durch die betroffene Person auf Maßnahmen nach Art. 32 DSGVO zugelassen wird, indem die Regelung gegenüber dem Verantwortlichen verbindliche Anforderungen zur Schaffung eines angemessenen Standards der Datensicherheit im Allgemeinen stellt (dazu unter 3.).

Die Vorgaben des Art. 32 DSGVO stehen somit zur Disposition der betroffenen Person.[12] Für den Verantwortlichen oder Auftragsverarbeiter enthalten sie dagegen verbindliche Regeln, da Art. 32 DSGVO eine Pflicht zur Implementierung angemessener Maßnahmen enthält und dem Verantwortlichen oder Auftragsverarbeiter gerade keine Entscheidungsbefugnis darüber einräumt, ob er diese umsetzt.[13]

[9] Vgl. zu § 9 BDSG und Art. 2 Abs. 1 iVm 1 Abs. 1 GG: Lotz/Wendler, CR 2016, 31, 34.
[10] Martini, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DSGVO Rn. 4b.
[11] Vgl. ErwGr. 10 S. 1 u 2 DSGVO.
[12] Ebenso Bay. Landesamt für Datenschutzaufsicht, Tätigkeitsbericht 2015/16, S. 99.
[13] Martini, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DSGVO Rn. 4c, der darauf abstellt, dass eine Einwilligung nur das Beziehungsgefüge betroffene Person - Verantwortlicher betrifft und nicht etwaige Dritte.

b. Stehen Art. 6 und 7 DSGVO der Abdingbarkeit von Schutzmaßnahmen entgegen?

Das systematische Argument, Art. 6 Abs. 1 lit. a und 7 DSGVO, die die Einwilligung regeln, beträfen nur das „Ob“ und nicht das “Wie“ der Verarbeitung und schlössen daher eine Einwilligung der betroffenen Person aus,[14] verfängt nicht.

Art. 6 Abs. 1 lit. a und 7 DSGVO schaffen die Rechtsgrundlage dafür, dass der Verantwortliche eine Verarbeitung überhaupt durchführen kann und setzen damit Art. 8 Abs. 2 GRCh um. Art. 6 und 7 DSGVO erweitern daher den Rechtskreis des Verantwortlichen, der ohne Rechtsgrundlage keine personenbezogenen Daten der betroffenen Person verarbeiten dürfte.

Die Einwilligung der betroffenen Person ist dabei eine Rechtsgrundlage unter vielen und ist Ausdruck der grundsätzlichen Dispositionsfreiheit der betroffenen Person über ihre Daten. Die übrigen Rechtsgrundlagen des Art. 6 Abs. 1 DSGVO (lit. b-f) schränken die Dispositionsfähigkeit der betroffenen Person dagegen ein. Aus der (grundrechtlich zwingend erforderlichen) Normierung dieser Rechtsgrundlagen, die gerade erst einen Eingriff in das Grundrecht aus Art. 8 GRCh erlauben, kann nicht geschlossen werden, dass die Dispositionsfreiheit der betroffenen Person nur soweit reicht wie sie in Art. 6 und 7 DSGVO geregelt ist. Die Dispositionsfreiheit der betroffenen Person ist vielmehr grundsätzlich unbeschränkt und wird durch Art. 6 DSGVO erst beschränkt.

Art. 6 und 7 DSGVO vergrößern also nicht den Rechtskreis der betroffenen Person, sondern allein den des Verantwortlichen. Die Rechte der betroffenen Person ergeben sich bereits aus Art. 8 GRCh und nicht erst aus der DSGVO. Aus Art. 6 Abs. 1 lit. a, 7 DSGVO kann daher lediglich der Schluss gezogen werden, dass die Dispositionsfreiheit der betroffenen Person nur soweit eingeschränkt werden kann, wie dies durch diese Normen vorgesehen ist. Der gegenteilige Schluss

[14] Jandt, in Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 32 DSGVO Rn. 40; Bescheid der österreichischen DSB, Az. D213.692/0001-DSB/2018 vom 16.11.18, 3.2., abrufbar unter https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=74ce9b96-f183-4bba-94e8-d17273ebf78b&Position=1&Sort=2%7cDesc&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=18.04.2019&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20181116_DSB_D213_692_0001_DSB_2018_00.
Zur Rechtslage nach § 9 S. 2 BDSG a.F.: Bergt, NJW 2011, 3752, 3755, der sich der Auffassung jedoch i.E. nicht anschließt.

darauf, dass Art. 6 und 7 DSGVO die Reichweite der Dispositionsfreiheit der betroffenen Person bestimmen, lässt sich der Gesetzessystematik nicht entnehmen.

Die Gesetzessystematik spricht daher – entgegen der eingangs dargestellten Literaturauffassung – gerade für die Möglichkeit der betroffenen Person in die Herabsetzung der Sicherheit der Verarbeitung einzuwilligen, da die Dispositionsfreiheit der betroffenen Person durch die Art. 6 und 7 DSGVO nur in Bezug auf das „Ob“ und nicht in Bezug auf das „Wie“ eingeschränkt wird. Da eine Regelung über eine Beschränkung der Dispositionsfreiheit über das „Wie“ fehlt, bleibt sie in Bezug auf das „Wie“ unbeschränkt.

Auch an dieser Stelle soll abschließend noch einmal die Konsequenz der Gegenauffassung aufgezeigt werden: Ließe man nur eine Einwilligung in das „Ob“ der Verarbeitung zu, wäre es möglich, darin einzuwilligen, dass die eigenen personenbezogenen Daten, auch Gesundheitsdaten, wie z.B. ein ärztliches Attest im Internet durch einen Dritten veröffentlicht werden. Nicht möglich wäre es aber darin einzuwilligen, dass der Dritte dieselben Daten per unverschlüsselter E-Mail an die betroffene Person verschickt, weil dann nicht garantiert werden kann, dass bei der Übermittlung nicht auf die Daten zugegriffen wird und sie vielleicht öffentlich bekannt würden. Dieses Ergebnis ist weder sachgerecht noch lässt es sich– wie gezeigt – aus den. Art. 6 Abs. 1 lit. a und 7 DSGVO ableiten.

c. Zwischenergebnis:

Die Einhaltung der Sicherheit der Verarbeitung bei einer konkreten Verarbeitung steht grundsätzlich zur Disposition der betroffenen Person.

3. Pflicht zur Schaffung der nach Art. 32 DSGVO erforderlichen Standards der Datensicherheit durch den Verantwortlichen oder Auftragsverarbeiter

Art. 25 Abs. 1 DSGVO verpflichtet den Verantwortlichen dazu „sowohl zum **Zeitpunkt der Festlegung der Mittel für die Verarbeitung** als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen“ zum Schutz der betroffenen Personen zu treffen. Das bedeutet, dass der Verantwortliche auch unabhängig von einer konkreten Verarbeitung aufgrund einer typisierenden Betrachtung der von ihm durchgeführten Verarbeitungen angemessene Schutzmaßnahmen zu ergreifen hat.[15]

Letzteres spiegelt sich auch darin wieder, dass Art. 32 DSGVO nicht von den Rechten und Freiheiten der einzelnen betroffenen Person spricht, sondern von den betroffenen Personen im Plural. Die Abwägung durch den Verantwortlichen hat also anhand einer typisierenden Abwägung stattzufinden, nicht bezogen auf die konkrete Einzelperson. Dies zeigt, dass Art. 32 DSGVO eine Pflicht für den Verantwortlichen oder Auftragsverarbeiter normiert, die von diesem zwingend umzusetzen ist. Da es sich nicht um die Daten des Verantwortlichen, sondern um die der betroffenen Person handelt, kann auch nur die betroffene Person über die Einhaltung der Vorgaben des Art. 32 DSGVO disponieren.

Eine freie Entscheidung über einen Verzicht der Einhaltung der Vorgaben des Art. 32 DSGVO kann die betroffene Person allerdings nur dann treffen, wenn die nach Art. 32 DSGVO erforderlichen TOMs durch den Verantwortlichen zumindest vorgehalten werden. Der Verantwortliche oder der Auftragsverarbeiter hat also schon zu dem Zeitpunkt, zu welchem er die Mittel für die spätere konkrete Verarbeitung festlegt, also beispielsweise, wenn er darüber entscheidet auf welchem Weg die Daten übertragen werden, die angemessenen technischen und organisatorischen Maßnahmen zu implementieren. Daher kann sich ein Verantwortlicher, der eine Verarbeitung durchführt, die die Übermittlung sensibler Daten erfordert, nicht darauf zurückziehen, dass er schon grundsätzlich keine sichere Übermittlung gewährleisten kann und dem Betroffenen eine pauschale Einwilligung dazu abringen. Vielmehr hat er eine sichere Übermittlungsform bereits zum Zeitpunkt der Auswahl der Mittel für die Verarbeitung vorzuhalten. Dies schließt nicht aus, dass der Betroffene in Bezug auf eine konkrete, ihn betreffende Verarbeitung darin einwilligen kann,

[15] Martini, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DSGVO Rn. 4c.

dass die konkrete Maßnahme ohne das nach Art. 32 DSGVO erforderliche Schutzniveau durchgeführt wird, vorausgesetzt, dass der Verantwortliche dieses grundsätzlich gewährleisten kann.[16]

Abschließend ist hervorzuheben, dass der spezielle Fall der Einwilligung in die unverschlüsselte E-Mail-Kommunikation mit Rechtsanwälten durch Einführung des § 2 Abs. 2 S. 5 BORA inzwischen **berufsrechtlich** legitimiert wurde. Die **datenschutzrechtliche Zulässigkeit** dieser Kommunikationsform bleibt durch § 2 Abs. 2 Satz 5 BORA allerdings unberührt, da es sich bei der DSGVO um gegenüber der BORA höherrangiges Europarecht handelt und keine Öffnungsklausel einschlägig ist.[17] Die BORA kann daher nur für das Berufsrecht Regelungen treffen, da dieses nicht in den Anwendungsbereich der DSGVO fällt, nicht jedoch für das Datenschutzrecht, welches insoweit abschließend durch die DSGVO geregelt ist. Daher gelten die hier gemachten Ausführungen auch für diesen Fall.[18]

Im Ergebnis ist Art. 32 DSGVO für den Verantwortlichen und den Auftragsverarbeiter zwingendes Recht. Diese haben die erforderlichen technischen Voraussetzungen zur Gewährleistung eines angemessenen Schutzniveaus vorzuhalten, auch wenn die Möglichkeit der betroffenen Person besteht, im Einzelfall auf entsprechende TOMs zu verzichten.

4. Voraussetzungen für eine wirksame Einwilligung

Aus den Ausführungen ergibt sich, dass eine Einwilligung in die Herabsetzung des Schutzniveaus möglich ist, allerdings nur unter zwei Voraussetzungen: Zum einen muss der Verantwortliche grundsätzlich in der Lage sein, das nach der Abwägung des Art. 32 DSGVO erforderliche Schutzniveau gewährleisten zu können. Zum anderen muss die Einwilligung den Anforderungen des Art. 7 DSGVO analog genügen.[19] Diese Voraussetzungen ergeben sich aus den unterschiedlichen Regelungswirkungen, die Art. 32 DSGVO gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter und der betroffenen Person entfaltet. Während Art. 32 DSGVO den Verantwortlichen unabhängig vom Einzelfall dazu verpflichtet, ein angemessenes Sicherheitsniveau bei den Verarbeitungen die er durchführt zu schaffen (dazu schon unter 3.), steht die Regelung der Freiheit der

[16] Martini, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DSGVO Rn. 4c.
[17] Gasteyer, AnwBlOnline 2019, 557, 558; Diese Auffassung teilt auch das BMJV: ZD-Aktuell 2020, 07039.
[18] Zur datenschutzrechtlichen Zulässigkeit der E-Mail-Kommunikation durch Anwälte: VG Mainz Urt. v. 17.12.2020 – 1 K 778/19.MZ, BeckRS 2020, 41220 Rn. 27- 40 und zur Abdingbarkeit in diesem Kontext: Römermann/Praß , in: BeckOK BORA, 30. Edition 2020, § 2 BORA Rn. 43 -44.
[19] I.E. auch Römermann/Praß, in: BeckOK BORA, Römermann 30. Edition, 2020, § 2 BORA Rn. 43 -44; Zur Freiwilligkeit der Einwilligung bei § 9 BDSG a.F.: Lotz/Wendler, CR 2016, 31, 35.

betroffenen Person darüber zu entscheiden, wie mit ihren Daten umgegangen wird, nicht entgegen (dazu schon unter 2.) Die DSGVO enthält mit Art. 7 DSGVO grundsätzliche Maßstäbe zur Beurteilung, wie eine Einwilligung der betroffenen Person zu gestalten ist. Diese beziehen sich zwar unmittelbar nur auf das „Ob“ der Verarbeitung, sind jedoch entsprechend auch auf das „Wie“ anzuwenden.[20] Die Einwilligung in die technische Umsetzung („Wie“) einer Verarbeitung ist sinnvollerweise nach denselben Maßstäben zu beurteilen wie die Frage, ob die Verarbeitung nach Art. 6 DSGVO zulässig ist („Ob“).[21] Die Wertungen des Art. 7 DSGVO und die damit verbundenen Anforderungen an die Einwilligung sollten nicht nur auf eine Teilfrage der Zulässigkeit der Verarbeitung bezogen werden, da die Verarbeitung als einheitlicher Vorgang - schon aus Gründen der Praktikabilität - betrachtet werden muss. Würde man an die Einwilligung in das „Ob“ und das „Wie“ unterschiedliche Maßstäbe anlegen, riefe dies erhebliche Abgrenzungsschwierigkeiten hervor und erwiese weder der betroffenen Person noch dem Verantwortlichen einen Dienst.

Voraussetzung jeder Abbedingung ist daher eine freiwillige Einwilligung; insbesondere muss der Betroffene frei von (auch faktischem) Zwang sein und eine echte Entscheidungsmöglichkeit haben. Er kann nicht gezwungen sein, einer unsicheren Datenverarbeitung zuzustimmen, wenn er einen Online-Dienst oder einen Arzt oder Rechtsanwalt seiner Wahl aufsucht. Vielmehr muss eine angemessene sichere Alternative für ihn bestehen, die er frei von unzumutbaren Nachteilen auswählen kann. So darf etwa, wenn als Alternative zu einem unverschlüsselten E-Mail-Versand die schriftliche Einreichung von Dokumenten angeboten wird, kein Zwang durch eine unangemessene Verlängerung der Bearbeitungsdauer oder durch Zusatzkosten ausgeübt werden. Eine Unzumutbarkeit kann sich aber auch daraus ergeben, dass Betroffene dauerhaft gezwungen sind, den aufwendigeren, zeitintensiveren und aufgrund von Druck- und Versandkosten kostenintensiveren Weg der schriftlichen Kommunikation zu wählen, weil keine sichere digitale Abwicklung ermöglicht wird. Der Verantwortliche hat deshalb von vornherein Sorge dafür zu tragen, dass auf konkret definierte und absehbare Zeit auch Möglichkeiten der sicheren digitalen Abwicklung eröffnet werden, die frei von diesen Nachteilen sind.

[20] Römermann/Praß , in: BeckOK BORA, 30. Edition 2020, § 2 BORA Rn. 44.
[21] Zu § 9 und 4a BDSG a.F. Bergt, NJW 2011, 3752, 3755.

5. Fazit

Der Verantwortliche und der Auftragsverarbeiter haben die nach Art. 32 DSGVO erforderlichen Maßnahmen zwingend umzusetzen und vorzuhalten. Betroffene Personen können in die Herabsetzung des nach Art. 32 DSGVO vorgesehenen Schutzniveaus allerdings bezogen auf ihre eigenen Daten im Einzelfall einwilligen, wenn die Einwilligung freiwillig im Sinne des Art. 7 DSGVO erfolgt. Dies setzt jedoch voraus, dass der Verantwortliche die nach Art. 32 DSGVO erforderlichen Schutzvorkehrungen grundsätzlich vorhält und der betroffenen Person auf Verlangen zur Verfügung stellt, ohne dass der betroffenen Person Nachteile dadurch entstehen.

J3, 18.2.21