

Erläuterungen

I. Allgemeiner Teil

Hauptgesichtspunkte des Entwurfs:

Anpassungen in den datenschutzrechtlichen Bestimmungen in den Dienstrechten an die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 04.05.2016 S. 1, (im Folgenden: DSGVO).

Im Übrigen wird auf die Ausführungen im Vorblatt verwiesen.

Finanzielle Auswirkungen

Es wird auf die Ausführungen in der WFA verwiesen.

Kompetenzgrundlage:

Die Zuständigkeit des Bundes zur Erlassung des vorgeschlagenen Bundesgesetzes ergibt sich

1. hinsichtlich der Art. 1 bis 4 (BDG 1979, GehG, VBG, RStDG), 7, 8 und 11 (B-GIBG, PG 1965 und PVG) aus Art. 10 Abs. 1 Z 16 B-VG (Dienstrecht und Personalvertretungsrecht der Bundesbediensteten),
2. hinsichtlich der Art. 5 (LDG 1984) aus Art. 14 Abs. 2 B-VG,
3. hinsichtlich der Art. 6 (LLDG 1985) aus Art. 14a Abs. 3 B-VG,
4. hinsichtlich der Art. 9 und 10 (BThPG und BB-PG) aus Art. 10 Abs. 1 Z 6 B-VG (Zivilrechtswesen),
5. hinsichtlich des Art. 12 (RPG) aus Art. 10 Abs. 1 Z 6 B-VG (Zivil- und Strafrechtswesen, Justizpflege, Angelegenheiten der Notarinnen und Notare, der Rechtsanwältinnen und Rechtsanwälte sowie verwandter Berufe).

II. Besonderer Teil

Zu § 48 Abs. 1, § 79e bis § 79h, § 204 Abs. 7, § 280 bis § 280b BDG 1979, § 171 GehG, § 3 Abs. 4, 96 und § 96a VBG, Artikel VI und § 3 Abs. 1 RStDG, § 6 Abs. 5 LDG 1984, § 6 Abs. 5 LLDG 1985, § 12 Abs. 2 und § 25 Abs. 6 B-GIBG, § 1a Abs. 1 bis 3, § 84, § 101 Abs. 1, 2 und 5, § 102 und § 105 Abs. 5 PG 1965, § 1a Abs. 1 bis 3, § 21 Abs. 1 und 2 und § 21a BThPG, § 1a Abs. 1 bis 3, § 68 Abs. 1 und 2 und § 69 BB-PG, § 9 Abs. 2 lit. f, n und o und Abs. 3 lit. i, n und o, § 10a Abs. 1 und 3 sowie § 14 Abs. 3 PVG und § 2 Abs. 3a sowie § 26a RPG:

Am 27. April 2016 wurde die DSGVO beschlossen. Die DSGVO ist am 25. Mai 2016 in Kraft getreten, tritt am 25. Mai 2018 in Geltung und hebt mit 25. Mai 2018 die Richtlinie 95/46/EG auf. Aus diesen Gründen sind Anpassungen in den datenschutzrechtlichen Bestimmungen der jeweiligen Materiengesetze erforderlich.

Die §§ 280 ff BDG 1979 und die weiteren datenschutzrechtlichen Bestimmungen sind als *leges speciales* zu den allgemeinen Regelungen des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999, in Zusammenschau mit diesem sowie der DSGVO zu lesen. Auf die Regelung des § 30 Abs. 5 DSG, wonach gegen Behörden und öffentliche Stellen keine Geldbußen verhängt werden können, darf an dieser Stelle hingewiesen werden. Bezüglich der Datenverarbeitung im Beschäftigungskontext wird von der Öffnungsklausel des Art. 88 DSGVO Gebrauch gemacht.

Der Anwendungsbereich der §§ 280 ff BDG 1979 erstreckt sich abweichend von § 1 BDG 1979 auf alle in § 280 Abs. 1 BDG 1979 genannten betroffenen Personen. Die §§ 280 ff BDG 1979 beziehen sich ausschließlich auf die erforderlichenfalls durch die Leiterinnen und Leiter der Zentralstellen als jeweils Verantwortliche verarbeiteten, übermittelten und weiterverarbeiteten personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien der in § 280 Abs. 1 BDG 1979 genannten betroffenen Personen. Diese Bestimmungen regeln also ausschließlich das Schicksal dieser durch die Leiterin oder den Leiter der jeweiligen Zentralstelle erforderlichenfalls verarbeiteten, übermittelten und weiterverarbeiteten dienstrechtlichen, arbeits- und sozialrechtlichen, haushaltsrechtlichen, besoldungsrechtlichen, pensionsrechtlichen, organisationsbezogenen, ausbildungsbezogenen und sonstigen mit den angeführten Rechtsverhältnissen in unmittelbarem Zusammenhang stehenden

personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien der betroffenen Personen.

Personenbezogene Daten oder personenbezogene Daten besonderer Kategorien von Personen gemäß § 280 Abs. 1 BDG 1979 stehen mit einem Rechtsverhältnis in unmittelbarem Zusammenhang, wenn diese Daten bei Außerachtlassung des Rechtsverhältnisses objektiv betrachtet nicht oder nicht in einer solchen Weise verarbeitet, übermittelt oder weiterverarbeitet werden würden, wie sie es bei Berücksichtigung des Rechtsverhältnisses werden würden. Beispielhaft können hierfür mit dem jeweiligen Rechtsverhältnis in unmittelbarem Zusammenhang stehende personenbezogene steuerrechtliche Daten angeführt werden. § 280 Abs. 1 und 2 BDG 1979 ermächtigt die Leiterinnen und Leiter der Zentralstellen als jeweils Verantwortliche lediglich, die im Beschäftigungskontext erforderlichen personenbezogenen Daten oder personenbezogenen Daten besonderer Kategorien zu verarbeiten, zu übermitteln und weiterzuverarbeiten.

Zu § 280 Abs. 1 und 2 BDG 1979 wird festgehalten, dass eine über die in diesen Absätzen festgelegten, eindeutigen und legitimen Zwecke hinausgehende Verarbeitung, Übermittlung und Weiterverarbeitung, sofern nicht ausdrücklich normiert, auf Grundlage des § 280 Abs. 1 und 2 BDG 1979 nicht vorgesehen ist. Von der Ermächtigung des § 280 Abs. 1 und 2 BDG 1979 sind lediglich erforderliche Übermittlungen zwischen den Leiterinnen und Leitern der Zentralstellen erfasst. Darüber hinausgehende Übermittlungen an Leiterinnen und Leiter der Zentralstellen oder Dritte bleiben von dieser Bestimmung unberührt und sind anhand ihrer jeweiligen Rechtsgrundlage zu beurteilen. Jedenfalls erforderlich ist eine Übermittlung, wenn ein Rechtsverhältnis in den Wirkungsbereich einer anderen Leiterin oder eines anderen Leiters einer Zentralstelle übergeht. Eine Weiterverarbeitung zu einem anderen Zweck, der ebenso wie der ursprüngliche Zweck der Verarbeitung von § 280 Abs. 2 BDG 1979 umfasst sein muss, ist nur möglich, sofern die personenbezogenen Daten oder die personenbezogenen Daten besonderer Kategorien zu diesem „neuen“ Zweck ebenfalls erhoben und verarbeitet werden dürften. Eine derartige neuerliche Erhebung bereits vorhandener Daten soll jedoch aus Gründen der Verwaltungsvereinfachung sowie den Grundsätzen der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit folgend unterbleiben, sofern eine Weiterverarbeitung erfolgen kann und darf.

§ 280 Abs. 3 BDG 1979 ermächtigt jeweils die Leiterinnen und Leiter der Zentralstellen, personenbezogene Daten und personenbezogene Daten besonderer Kategorien gemäß § 280 Abs. 1 BDG 1979 ausschließlich auf Ersuchen einer zuständigen Behörde, deren Aufgabe die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, die Strafvollstreckung oder der Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit ist, unter den im Gesetz angeführten Voraussetzungen zu verarbeiten. Beispielhaft können als zuständige Behörden kriminalpolizeiliche Behörden oder Justizbehörden, insbesondere Staatsanwaltschaften oder Gerichte, genannt werden. Die Beschränkung der Rechte der betroffenen Person im notwendigen und verhältnismäßigen Ausmaß erfolgt gemäß Art. 23 DSGVO, liegt im allgemeinen öffentlichen Interesse und stellt sicher, dass die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit gewährleistet ist. Die zuständige Behörde soll durch die Vornahme der erforderlichen bloßen Verarbeitung durch die Leiterin oder den Leiter der jeweiligen Zentralstelle unterstützt werden. Die Information an die betroffene Person hat nach Mitteilung durch die ersuchende zuständige Behörde an die Leiterin oder den Leiter der jeweiligen Zentralstelle direkt zu erfolgen, was bedeutet, dass es zu keiner Befassung von Zwischenvorgesetzten kommen soll. § 280 Abs. 3 BDG 1979 regelt ausschließlich die bloße Verarbeitung aufgrund eines Ersuchens zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, der Strafvollstreckung oder dem Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Sonstige Ersuchen sind gemäß § 280 Abs. 1 und 2 BDG 1979 oder gemäß ihrer jeweiligen Rechtsgrundlage zu beurteilen.

Da Art. 37 bis 39 DSGVO insbesondere die Stellung sowie die Aufgaben einer oder eines Datenschutzbeauftragten regeln, ist in § 280 Abs. 4 BDG 1979 nur noch die formale Zuständigkeit zur Benennung festzulegen. Auf § 5 DSG wird hingewiesen. Wird von den Leiterinnen und Leitern der Zentralstellen jeweils für den Wirkungsbereich des jeweiligen Ressorts nicht eine (gemeinsame) Datenschutzbeauftragte oder ein (gemeinsamer) Datenschutzbeauftragter, sondern werden mehrere Datenschutzbeauftragte benannt, so soll klargestellt sein, dass dies nur nötigenfalls und stets unter dem Aspekt der Aufteilung der Zuständigkeit für den Wirkungsbereich des jeweiligen Ressorts erfolgen soll, sodass auch in diesem Fall stets die Zuständigkeit einer oder eines benannten Datenschutzbeauftragten gegeben ist.

§ 280 Abs. 5 BDG 1979 regelt zusätzlich zur bereits bestehenden Einsichtsermächtigung der Bundesministerin oder des Bundesministers für öffentlichen Dienst und Sport im Rahmen der ihr oder ihm in Vorschriften gemäß § 280 Abs. 2 Z 2 BDG 1979 übertragenen Mitwirkungsbefugnisse die erforderliche nicht datenändernde Verarbeitung, Übermittlung und Weiterverarbeitung der genannten

Daten auch zum Zwecke der Sicherung der Datenqualität. Nicht datenändernd bedeutet, dass durch die Verarbeitungen, Übermittlungen und Weiterverarbeitungen die in den Personaldatensystemen gemäß § 280 Abs. 1 BDG 1979 erfassten personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien nicht verändert werden. So sollen etwaige im Zuge der Einsichtnahme auftauchende unklare oder missverständliche Daten erforderlichenfalls untersucht und durch entsprechende Mitteilung an den jeweiligen Verantwortlichen oder die jeweils gemeinsam Verantwortlichen durch diesen oder diese einer Klarstellung zugeführt werden können.

Gemäß § 280 Abs. 6 BDG 1979 ist die Bundesministerin oder der Bundesminister für öffentlichen Dienst und Sport ermächtigt, personenbezogene Daten und personenbezogene Daten besonderer Kategorien zusätzlich zur bereits bestehenden Regelung zu statistischen Auswertungen auch zu wissenschaftlichen oder historischen Forschungszwecken unter den angeführten Voraussetzungen zu verarbeiten, zu übermitteln und weiterzuverarbeiten. Soweit hierbei personenbezogene Daten besonderer Kategorien verarbeitet, übermittelt oder weiterverarbeitet werden, muss ein schriftlich zu dokumentierendes wichtiges öffentliches Interesse an der Untersuchung vorliegen. In § 280 Abs. 6 dritter Satz BDG 1979 wird von der Öffnungsklausel in Art. 89 Abs. 2 DSGVO Gebrauch gemacht und werden die in den Art. 15, 16, 18 und 21 DSGVO angeführten Rechte der betroffenen Personen im Rahmen einer Abwägung im jeweiligen Einzelfall beschränkt. Dadurch soll insbesondere sichergestellt werden, dass die für diese Zwecke notwendige Vollständigkeit der Daten gewährleistet und nicht durch Ausübung der genannten Rechte der betroffenen Personen ernsthaft beeinträchtigt oder unmöglich gemacht wird. Regelungen zur Auflösung des Personenbezuges durch geeignete technische Mittel tragen insbesondere dem Grundsatz der Datenminimierung Rechnung. Erforderlichenfalls ist die Bundesministerin oder der Bundesminister für öffentlichen Dienst und Sport abermals ermächtigt, nicht datenändernde Verarbeitungen, Übermittlungen und Weiterverarbeitungen der genannten Daten auch zum Zwecke der Sicherung der Datenqualität vorzunehmen. Nicht datenändernd bedeutet, dass durch die Verarbeitungen, Übermittlungen und Weiterverarbeitungen die in den Personaldatensystemen gemäß § 280 Abs. 1 BDG 1979 erfassten personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien nicht verändert werden. So sollen etwaige im Zuge einer beispielsweise statistischen Auswertung auftauchende unklare oder missverständliche Daten erforderlichenfalls untersucht und durch entsprechende Mitteilung an den jeweiligen Verantwortlichen oder die jeweils gemeinsam Verantwortlichen durch diesen oder diese einer Klarstellung zugeführt werden können.

§ 280 Abs. 7 BDG 1979 regelt die bereits bestehende Ermächtigung der Bundesministerin oder des Bundesministers für öffentlichen Dienst und Sport zur Verarbeitung, Übermittlung und Weiterverarbeitung von Adressdaten für Benachrichtigungen und Befragungen unter den angeführten Voraussetzungen sowie im Rahmen der vorzunehmenden Abwägung. Eine Verarbeitung, Übermittlung und Weiterverarbeitung gemäß dieser Bestimmung hat ausschließlich zum Zwecke der Benachrichtigung oder Befragung der betroffenen Personen zu erfolgen. Durch die zu berücksichtigenden Aspekte soll vor allem verhindert werden, dass zum Beispiel durch die Auswahl eines bestimmten Personenkreises für eine Benachrichtigung oder Befragung Rückschlüsse auf personenbezogene Daten oder personenbezogene Daten besonderer Kategorien möglich sind.

Aufgrund der umfassenden Neuregelung der Datenverarbeitung in den §§ 280 bis 280b BDG 1979 können § 171 GehG, § 96 VBG, Artikel VI RStDG und § 26a RPG entfallen.

In § 280a Abs. 1 BDG 1979 erfolgt eine Anpassung des Personenkreises an § 280 Abs. 1 BDG 1979, weswegen § 96a VBG entfallen kann.

§ 280a Abs. 2 bis 5 BDG 1979 enthält Bestimmungen zur Datenaufbewahrung. Bei gemeinsam Verantwortlichen ist dem Grundsatz der Datenminimierung folgend die Aufbewahrungspflicht nur von einem Verantwortlichen wahrzunehmen. Gesetzlich ist eine fünfzehnjährige Frist für personenbezogene Daten und personenbezogene Daten besonderer Kategorien vorgesehen. Für Protokolldaten über lesende Zugriffe ist eine dreijährige Frist und für Protokolldaten über datenändernde Zugriffe eine siebenjährige Frist vorgesehen. Diese Fristen ergeben sich aus einer Abwägung, die vor allem das Grundrecht auf Datenschutz, das Grundrecht auf Achtung des Privat- und Familienlebens, die Rechenschaftspflicht des jeweils Verantwortlichen, den Grundsatz der Integrität und Vertraulichkeit, den Grundsatz der Speicherbegrenzung, den Grundsatz der Datenminimierung, die Grundsätze der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit, die verschiedenen Verjährungsfristen, das öffentliche Interesse, insbesondere im Hinblick auf den rechtskonformen Vollzug der Gesetze, die Erfüllung der Kernaufgaben des Staates, die Aufrechterhaltung und das ordnungsgemäße Funktionieren des Öffentlichen Dienstes sowie dessen Nachvollziehbarkeit, die bereits vorgefundene Wertung strafrechtlich geschützter Rechtsgüter sowie den Beschäftigungskontext berücksichtigt.

§ 280a Abs. 6 BDG 1979 bestimmt, dass eine durch Gesetz oder Verordnung vorgesehene längere Aufbewahrungspflicht oder Archivierung den in § 280 Abs. 2 bis 5 BDG 1979 vorgesehenen Aufbewahrungspflichten vorgeht. Etwaige längere Aufbewahrungspflichten sollen demnach nicht durch die Einführung einer Aufbewahrungspflicht gemäß § 280a BDG 1979 verkürzt werden. Ebenso unberührt bleiben soll die Löschpflicht von Strafregistrauskünften. Werden jedoch speziellere Fristen für Aufbewahrungspflichten durch den Verantwortlichen oder die gemeinsam Verantwortlichen mittels Verordnung vorgesehen, so gehen diese der jeweiligen Frist der Aufbewahrungspflicht gemäß § 280a Abs. 2 bis 5 BDG 1979 vor. Die Fristen für Protokolldaten über lesende Zugriffe müssen jedoch mindestens ein Jahr und für Protokolldaten über datenändernde Zugriffe mindestens drei Jahre betragen, damit insbesondere die Rechte betroffener Personen nicht durch zu kurze Fristen eingeschränkt werden. Eine durch Gesetz oder Verordnung vorgesehene längere Frist einer Aufbewahrungspflicht oder Archivierung geht gemäß § 280 Abs. 6 BDG 1979 auch einer durch Verordnung gemäß § 280a Abs. 7 BDG 1979 festgesetzten kürzeren Frist vor. Gemeinsam Verantwortliche haben beim Erlassen einer Verordnung gemäß § 280a Abs. 7 BDG 1979 das Einvernehmen herzustellen. Durch die Verordnungsermächtigung in § 280a Abs. 7 BDG 1979 soll insbesondere den Grundsätzen der Speicherbegrenzung und Datenminimierung besonders Rechnung getragen werden.

§ 280a Abs. 7 BDG 1979 ermächtigt die Bundeskanzlerin oder den Bundeskanzler erforderlichenfalls zur nicht datenändernden Verarbeitung, Übermittlung und Weiterverarbeitung der genannten Daten, damit in Bezug auf die IKT-Lösungen und IT-Verfahren für das Personalmanagement des Bundes die Verfahren rechtskonform gestaltet, Fehler behoben und die Datensicherheit gewährleistet werden können. Die Erforderlichkeit der Verarbeitung, Übermittlung und Weiterverarbeitung personenbezogener Daten und personenbezogener Daten besonderer Kategorien zu den genannten Zwecken ist eng auszulegen. Datensicherheit bezieht sich nicht nur auf den physischen Zugang zu den Personaldatensystemen, sondern bedeutet auch, dass sichergestellt wird, dass die IKT-Lösungen und IT-Verfahren für das Personalmanagement des Bundes Verarbeitungen, Übermittlungen und Weiterverarbeitungen von personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien nur berechtigten Personen ermöglichen und diese Daten nur berechtigten Personen zur Verfügung stehen. Personenbezogene Daten und personenbezogene Daten besonderer Kategorien sind vor unrechtmäßigen Verarbeitungen, Übermittlungen oder Weiterverarbeitungen zu schützen, was insbesondere durch entsprechende Protokollierung zu erfolgen hat. Daher ist von dem oder den jeweils Verantwortlichen sicherzustellen, dass bestehende Protokolldaten nicht verändert werden können. Für Bereiche, in denen die Leiterinnen und Leiter der Zentralstellen jeweils mit der Bundeskanzlerin oder dem Bundeskanzler gemeinsam Verantwortliche sind, erfolgt gemäß § 280b Abs. 2 BDG 1979 die Aufteilung der Pflichten unbeschadet der Stellung als gemeinsam Verantwortliche im Sinne der DSGVO durch die von der Bundesregierung durch Verordnung zu erlassenden Verfahrensvorschriften. Die Möglichkeit zur Festlegung der jeweiligen Aufgaben der Verantwortlichen durch Rechtsvorschriften der Mitgliedstaaten, denen die Verantwortlichen unterliegen, wird in Art. 26 Abs. 1 DSGVO eröffnet. Dadurch soll vor allem gewährleistet sein, dass betroffene Personen bei der Geltendmachung ihrer Rechte gemäß DSGVO hinsichtlich standardisierter IKT-Lösungen und IT-Verfahren des Personalmanagement des Bundes unabhängig davon, welche Konstellation gemeinsam Verantwortlicher vorliegt, vergleichbar behandelt werden.

§ 280b Abs. 4 BDG 1979 sieht für die Ausübung der Rechte nach der DSGVO einen Identitätsnachweis vor. Ein solcher muss zweifelsfrei erkennen lassen, wer die betroffene Person ist, die ihre Rechte ausübt. Im Unzuständigkeitsfall ist die betroffene Person an den zuständigen Verantwortlichen zu verweisen. Die entsprechenden Informationen haben sodann auf direktem Weg von der Dienstbehörde oder Personalstelle an die betroffene Person zu ergehen. Direkt bedeutet, dass es dabei zu keiner Befassung von Zwischenvorgesetzten kommen soll. Es wird auf Art. 12 DSGVO verwiesen, der die transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der Betroffenen regelt. Für eine Verlängerung der Frist ist von Bedeutung, dass die betroffene Person vor Ablauf der Monatsfrist verständigt wird. Eine solche Verständigung hat jedenfalls eine Information über die Fristverlängerung und eine entsprechende Begründung zu enthalten.

In § 280b Abs. 5 bis 8 BDG 1979 wird von der in Art. 23 DSGVO eröffneten Möglichkeit der Beschränkung der Pflichten und Rechte gemäß Art. 5, 12 bis 22 und 34 DSGVO Gebrauch gemacht. Dies erfolgt unter Beachtung des Wesensgehalts der Grundrechte und Grundfreiheiten und stellt eine notwendige und verhältnismäßige Maßnahme dar. Derartige Beschränkungen von Rechten und Pflichten müssen darüber hinaus der Sicherstellung bestimmter Zwecke dienen, unter denen beispielsweise in Art. 23 Abs. 1 lit. e DSGVO der „Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und

Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit“ genannt wird. Daneben können sich solche Beschränkungen beispielsweise auch auf Art. 23 Abs. 1 lit. h bis j DSGVO stützen. Die Verarbeitung, Übermittlung und Weiterverarbeitung von personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien ist für den Öffentlichen Dienst unerlässlich und liegt aufgrund des überwiegenden, berechtigten öffentlichen Interesses an der Aufrechterhaltung und dem ordnungsgemäßen und rechtskonformen Funktionieren des Öffentlichen Dienstes, insbesondere im Sinne einer Erfüllung der Kernaufgaben des Staates unter Wahrung der Grundsätze der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit, selbst im öffentlichen Interesse. Insbesondere ist es erforderlich, dass im Öffentlichen Dienst weiterhin die Möglichkeit zur Dienstaufsicht sowie zur Planstellenbewirtschaftung besteht und dass die Revisionsicherheit gewährleistet ist. Es ist daher erforderlich und sachgerecht, gewisse Beschränkungen der Rechte der betroffenen Personen vorzunehmen.

§ 280b Abs. 5 BDG 1979 schließt das Recht auf Berichtigung gemäß Art. 16 DSGVO bei unrichtigen oder unvollständigen personenbezogenen Daten oder personenbezogenen Daten besonderer Kategorien aus, wenn einer solchen Berichtigung die Rechtskraft oder die Verjährung entgegenstehen, oder wenn ein zumutbarer Rechtsweg besteht oder bestand. Damit ist klargestellt, dass das Recht auf Berichtigung auch im Anwendungsbereich der §§ 280 ff BDG 1979 nicht der Umgehung anderer rechtlicher Vorschriften dient.

§ 280b Abs. 6 BDG 1979 schließt das Recht auf Löschung gemäß Art. 17 DSGVO für Zeiten einer durch Gesetz oder Verordnung vorgesehenen Aufbewahrungspflicht oder Archivierung aus. Eine solche Möglichkeit besteht gemäß Art. 17 Abs. 3 DSGVO zur Erfüllung einer rechtlichen Verpflichtung, wie beispielsweise einer Aufbewahrungspflicht, die die Verarbeitung nach dem Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Zur Aufrechterhaltung des Öffentlichen Dienstes und der öffentlichen Ordnung und Sicherheit als allgemeines öffentliches Interesse und zur Sicherstellung der mit der Verarbeitung, Übermittlung und Weiterverarbeitung personenbezogener Daten und personenbezogener Daten besonderer Kategorien von betroffenen Personen verbundenen Kontroll-, Überwachungs- und Ordnungsfunktion ist die gesetzlich vorgesehene Verarbeitung, Übermittlung und Weiterverarbeitung der genannten Daten bis zum Ablauf der durch Gesetz oder durch Verordnung bestimmten Frist der Aufbewahrungspflicht erforderlich. Auf Art. 17 Abs. 3 lit. d und e DSGVO wird außerdem hingewiesen.

§ 280b Abs. 7 BDG 1979 regelt eine erforderliche und sachgerechte Beschränkung des Rechtes auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO. Die Überprüfung der Richtigkeit der personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien der betroffenen Person soll nämlich nicht dazu führen, dass in den standardisierten IKT-Lösungen und IT-Verfahren für das Personalmanagement des Bundes die Verarbeitung, Übermittlung und Weiterverarbeitung einzuschränken wäre, was beispielsweise ein momentanes Anhalten der Vorrückung oder eine nicht zeitgerechte Anweisung des zustehenden Bezuges zur Folge haben kann. Alleine das Bestehen dieser möglichen Folgen aufgrund der integrierten Systeme würde neben der Verursachung eines beträchtlichen Verwaltungsaufwandes für viele betroffene Personen die Geltendmachung ihrer Rechte gemäß DSGVO erschweren oder faktisch unmöglich machen, weswegen für den Anwendungsbereich der §§ 280 ff BDG 1979 eine Beschränkung des Rechtes auf Einschränkung der Verarbeitung im erforderlichen Ausmaß vorgeschlagen wird. Gleiches gilt für den Zeitraum, in dem die betroffene Person ihr Recht auf Widerspruch geltend gemacht hat und noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen. Eine Beschränkung des Rechtes auf Einschränkung der Verarbeitung ist auch im Lichte des wichtigen wirtschaftlichen und finanziellen Interesses des Staates, beispielsweise im Haushalts- und Steuerbereich, erforderlich und sachgerecht im Sinne des Art. 23 Abs. 1 DSGVO, da etwa die rechtskonforme Abführung von Beiträgen zur Sozialversicherung und der Lohnsteuer ein wichtiges Ziel des allgemeinen öffentlichen Interesses darstellt, dessen Schutz die Beschränkung von Rechten rechtfertigt.

Aufgrund des überwiegenden, berechtigten öffentlichen Interesses an der Verarbeitung der personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien der Personen gemäß § 280 Abs. 1 BDG 1979 ist es erforderlich und sachgerecht, das Recht auf Widerspruch gemäß Art. 21 DSGVO in § 280b Abs. 8 BDG 1979 für Zeiten einer durch Gesetz oder Verordnung vorgesehenen Aufbewahrungspflicht oder Archivierung auszuschließen. Die Erforderlichkeit und Sachlichkeit dieser Beschränkung ergibt sich ebenfalls aus dem überwiegenden, berechtigten öffentlichen Interesse an der Aufrechterhaltung und dem ordnungsgemäßen Funktionieren des Öffentlichen Dienstes, konkret dem rechtskonformen Vollzug der Personaladministration und dem rechtskonformen Abführen von Beiträgen, beispielsweise zur Sozialversicherung und der Lohnsteuer. Verarbeitungen, Übermittlungen und

Weiterverarbeitungen gemäß § 280 Abs. 1 BDG 1979 erfolgen ausschließlich zu in § 280 Abs. 2 BDG 1979 genannten Zwecken, sofern dies erforderlich ist. Auch für die weiteren Verarbeitungen, Übermittlungen und Weiterverarbeitungen gemäß den §§ 280 und 280a Abs. 1 und 7 BDG 1979 besteht ein überwiegendes, berechtigtes öffentliches Interesse, wobei auch auf Art. 21 Abs. 6 DSGVO hingewiesen wird. Darüber hinaus würde für den Fall, dass eine betroffene Person ihr Recht auf Widerspruch geltend macht, eine weitere Verarbeitung, Übermittlung und Weiterverarbeitung erforderlich werden, was dem grundsätzlichen Anliegen der betroffenen Person zuwiderlaufen würde. Es wird daher eine sachgerechte und erforderliche Beschränkung des Rechtes auf Widerspruch gemäß Art. 21 DSGVO im Sinne des Art. 23 DSGVO für Zeiten einer durch Gesetz oder Verordnung vorgesehenen Aufbewahrungspflicht oder Archivierung vorgeschlagen.

In § 79e BDG 1979 wird neben terminologischen Anpassungen eine Abwägung der Verarbeitung im Falle der Erforderlichkeit mit den Interessen oder den Grundrechten und Grundfreiheiten vorgesehen. Personenbezogene Daten oder personenbezogene Daten besonderer Kategorien der IKT-Nutzung dürfen gemäß § 79e Abs. 2 BDG 1979 nach Maßgabe der §§ 79f und 79g BDG 1979 zu Kontrollzwecken nur verwendet werden, wenn dies zu einem der angeführten Zwecke erforderlich ist sowie im Rahmen einer Abwägung. Eine solche Abwägung ist nunmehr auch in § 79e Abs. 3 BDG 1979 vorgesehen. Kontrollmaßnahmen dürfen sich gemäß § 79e Abs. 4 BDG 1979 wegen des Grundsatzes der Datenminimierung nur auf die unbedingt erforderliche Anzahl an Bediensteten beziehen.

In § 79f BDG 1979 werden terminologische Anpassungen an die DSGVO vorgenommen, in § 79f Abs. 3 BDG 1979 das Schriftlichkeitserfordernis für die Dokumentation eingeführt und in § 79f Abs. 5 BDG 1979 der Fall einer konkreten unmittelbaren Gefährdung für die IKT-Infrastruktur und ihre korrekte Funktionsfähigkeit aufgrund einer IKT-Nutzung an das neue Datenschutzrecht angepasst, wobei ebenfalls eine Abwägung vorgesehen ist. Protokolldaten sind der Beamtin oder dem Beamten auf ihr oder sein Verlangen direkt, also ohne Befassung von Zwischenvorgesetzten, zur Verfügung zu stellen.

Gleiches gilt für § 79g Abs. 1 und 7 BDG 1979, wobei im ersten Fall die Verarbeitung zur Aufdeckung einer gröblichen Dienstpflichtverletzung ohne und im zweiten Fall mit einem gegen eine bestimmte Beamtin oder einen bestimmten Beamten gerichteten Verdacht geregelt wird. In § 79g Abs. 4 BDG 1979 wird im Sinne der Rechenschaftspflicht das Einführen des Schriftlichkeitserfordernisses für die Dokumentation vorgesehen. § 79g Abs. 7 BDG 1979 verweist nunmehr nicht mehr auf § 79e Abs. 1 BDG 1979, weil die dort angeführte Abwägung auch in diesem Fall der Verarbeitung zur Anwendung gelangen soll. Auch der Verweis auf § 79e Abs. 4 BDG 1979 kann entfallen, weil sich dieser nunmehr auf die unbedingt erforderliche Anzahl an Bediensteten bezieht. Dass die Beamtin oder der Beamte von der Leiterin oder dem Leiter der Dienststelle umgehend direkt über den Bericht der IT-Stelle und den diesem vorausgegangenen Ermittlungsauftrag zu informieren ist bedeutet auch hier, dass die Information ohne Befassung von Zwischenvorgesetzten an die betroffene Person ergehen soll.

§ 48 Abs. 1 und § 79h BDG 1979, § 12 Abs. 2 und § 25 Abs. 6 B-GIBG, § 1a Abs. 1 bis 3, § 84, § 101 Abs. 1, 2 und 5, § 102 und § 105 Abs. 5 PG 1965, § 1a Abs. 1 bis 3, § 21 Abs. 1 und 2 und § 21a BThPG, § 1a Abs. 1 bis 3, § 68 Abs. 1 und 2 und § 69 BB-PG und § 9 Abs. 2 lit. f, n und o sowie Abs. 3 lit. i, n und o, § 10a und § 14 Abs. 3 PVG werden terminologisch an das neue Datenschutzrecht angepasst.

In § 204 Abs. 7 BDG 1979, § 3 Abs. 4 VBG, § 3 Abs. 1 RStDG, § 6 Abs. 5 LDG 1984, § 6 Abs. 5 LLDG 1985 und § 2 Abs. 3a RPG werden zusätzlich zur Klarstellung, dass die jeweilige Verarbeitung im Sinne der Rechenschaftspflicht schriftlich dokumentiert zu erfolgen hat, terminologische Anpassungen an das neue Datenschutzrecht vorgenommen. Neben der Prüfung etwaiger Zulassungserfordernisse sind vor allem die Einholung und Verarbeitung von Strafregistereinkünften gemäß den §§ 9 und 9a des Strafregistergesetzes 1968, BGBl. Nr. 277/1968, sowie die Abfrage und Verarbeitung von Vorwarnungen nach Art. 56a der Richtlinie 2005/36/EG über die Anerkennung von Berufsqualifikationen, ABl. Nr. L 255 vom 30.09.2005 S. 22, zuletzt berichtigt durch ABl. Nr. L 305 vom 24.10.2014 S. 115, zuletzt geändert durch die Richtlinie 2013/55/EU, ABl. Nr. L 354 vom 28.12.2013 S. 132, (im Folgenden: Richtlinie 2005/36/EG) im Binnenmarkt-Informationssystem (IMI) vorgesehen. Diese dienen primär dienstrechtlichen Zwecken und werden von Stellen durchgeführt, deren Hauptaufgaben nicht im Bereich der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten liegen, weswegen der Anwendungsbereich der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. Nr. L 119 vom 04.05.2016 S. 89, ebenso wie bei der bloßen Verarbeitung von Daten zu Strafverfolgungszwecken wie im Falle des § 280 Abs. 3 BDG 1979 nicht eröffnet ist.

DATENSCHUTZ-FOLGENABSCHÄTZUNG

SYSTEMATISCHE BESCHREIBUNG

der geplanten Verarbeitungsvorgänge, Zwecke sowie berechtigten Interessen

Die Leiterinnen und Leiter der Zentralstellen sind ermächtigt, personenbezogene Daten und personenbezogene Daten besonderer Kategorien der Personen gemäß § 280 Abs. 1 BDG 1979 im Sinne des Art. 4 Z 2 DSGVO zu verarbeiten, einander zu übermitteln und zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, zu verarbeiten (Weiterverarbeitung). Eine solche Verarbeitung, Übermittlung oder Weiterverarbeitung muss entweder zum Zwecke der Aufrechterhaltung oder des Funktionierens des Öffentlichen Dienstes, oder zum Zwecke der Erfüllung der rechtlichen Verpflichtungen oder der Geltendmachung der Rechte, die sich aus den in § 280 Abs. 2 Z 2 BDG 1979 genannten Vorschriften ergeben, oder gemäß § 280 Abs. 2 Z 3 BDG 1979 zum Zwecke der Ausübung der in den Vorschriften gemäß § 280 Abs. 2 Z 2 BDG 1979 übertragenen öffentlichen Gewalt erforderlich sein. Eine über die in diesen Absätzen festgelegten, eindeutigen und legitimen Zwecke hinausgehende Verarbeitung, Übermittlung oder Weiterverarbeitung ist, sofern nicht ausdrücklich normiert, gemäß § 280 Abs. 1 und 2 BDG 1979 nicht vorgesehen.

§ 280 Abs. 3 BDG 1979 ermächtigt die Leiterinnen und Leiter der Zentralstellen, personenbezogene Daten und personenbezogene Daten besonderer Kategorien gemäß § 280 Abs. 1 BDG 1979 auf Ersuchen einer zuständigen Behörde, deren Aufgabe die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, die Strafvollstreckung oder der Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit ist, unter den im Gesetz angeführten Voraussetzungen zu verarbeiten.

§ 280 Abs. 5 BDG 1979 ermächtigt die Bundesministerin oder den Bundesminister für öffentlichen Dienst und Sport, soweit dies zum Zwecke der Wahrnehmung der ihr oder ihm in Vollziehung dieses Bundesgesetzes oder anderer in § 280 Abs. 2 Z 2 BDG 1979 genannter Vorschriften übertragenen Mitwirkungsbefugnisse erforderlich ist, in die von § 280 Abs. 1 BDG 1979 erfassten Personaldatensysteme direkt Einsicht zu nehmen und im Einzelfall erforderlichenfalls nicht datenändernde Verarbeitungen, Übermittlungen und Weiterverarbeitungen auch zum Zwecke der Sicherung der Datenqualität vorzunehmen.

§ 280 Abs. 6 BDG 1979 ermächtigt die Bundesministerin oder den Bundesminister für öffentlichen Dienst und Sport, personenbezogene Daten und personenbezogene Daten besonderer Kategorien zusätzlich zur bereits bestehenden Regelung zu statistischen Auswertungen auch zu wissenschaftlichen oder historischen Forschungszwecken unter den angeführten Voraussetzungen zu verarbeiten, zu übermitteln und weiterzuverarbeiten. Soweit hierbei personenbezogene Daten besonderer Kategorien verarbeitet werden, muss ein schriftlich zu dokumentierendes wichtiges öffentliches Interesse an der Untersuchung vorliegen.

In § 280 Abs. 6 dritter Satz BDG 1979 wird jeweils von der Öffnungsklausel in Art. 89 Abs. 2 DSGVO Gebrauch gemacht und werden die in den Art. 15, 16, 18 und 21 DSGVO angeführten Rechte der betroffenen Personen im Rahmen einer Abwägung beschränkt. Dadurch soll insbesondere sichergestellt werden, dass die für die statistischen Zwecke oder die wissenschaftlichen oder historischen Forschungszwecke notwendige Vollständigkeit der Daten gewährleistet und nicht durch Ausübung der genannten Rechte der betroffenen Personen ernsthaft beeinträchtigt oder unmöglich gemacht wird. Regelungen zum unverzüglichen Auflösen des Personenbezuges durch geeignete technische Mittel tragen den Grundsätzen der Datenminimierung und Speicherbegrenzung Rechnung. Erforderlichenfalls ist die Bundesministerin oder der Bundesminister für öffentlichen Dienst und Sport ermächtigt, im Einzelfall auch nicht datenändernde Verarbeitungen, Übermittlungen und Weiterverarbeitungen zum Zwecke der Sicherung der Datenqualität vorzunehmen.

Gemäß § 280 Abs. 7 BDG 1979 ist die Bundesministerin oder der Bundesminister für öffentlichen Dienst und Sport ermächtigt, unter den angeführten Voraussetzungen erforderlichenfalls aus den von § 280 Abs. 1 BDG 1979 erfassten Personaldatensystemen Adressdaten für Benachrichtigungen oder Befragungen zu verarbeiten, zu übermitteln und weiterzuverarbeiten.

§ 280a Abs. 1 BDG 1979 sieht zum Zwecke der eindeutigen Identifikation im Beschäftigungskontext die Möglichkeit der elektronischen Personenkennzeichnung der in § 280 Abs. 1 BDG 1979 angeführten Personen vor.

Zur Erfüllung der Aufbewahrungspflicht gemäß § 280a Abs. 2 bis 5 BDG 1979 sind die jeweiligen Verantwortlichen gemäß § 280a Abs. 6 BDG 1979 ermächtigt, im Zentralen Personenstandsregister Abfragen der eingetragenen Todesfälle und Todeserklärungen durchzuführen.

§ 280a Abs. 7 ermächtigt die Bundeskanzlerin oder den Bundeskanzler, zum Zwecke der rechtskonformen Verfahrensgestaltung, der Fehlerbehebung sowie der Datensicherheit in den von ihr

oder ihm bereitgestellten oder betriebenen IKT-Lösungen und IT-Verfahren für das Personalmanagement des Bundes erforderliche nicht datenändernde Verarbeitungen, Übermittlungen und Weiterverarbeitungen von personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien durchzuführen.

Im 5a. Unterabschnitt des BDG 1979 wird die Nutzung der Informations- und Kommunikationstechnologie oder -technik (IKT) geregelt, die insbesondere die Kontrolle zur Abwehr von Schäden an der IKT-Infrastruktur und zur Gewährleistung ihrer korrekten Funktionsfähigkeit (vgl. § 79f BDG 1979), die Kontrolle bei begründetem Verdacht einer gröblichen Dienstpflichtverletzung (vgl. § 79g BDG 1979) sowie sonstige zulässige Datenverarbeitungen (vgl. § 79h BDG 1979) umfasst.

§ 204 Abs. 7 BDG 1979, § 3 Abs. 4 VBG, § 3 Abs. 1 RStDG, § 6 Abs. 5 LDG 1984, § 6 Abs. 5 LLDG 1985 und § 2 Abs. 3a RPG regeln die Verarbeitung personenbezogener Daten und personenbezogener Daten besonderer Kategorien durch die jeweilige Dienstbehörde oder Personalstelle. Neben der Prüfung etwaiger Zulassungserfordernisse sind vor allem die Einholung und Verarbeitung von Strafregistereinkünften gemäß den §§ 9 und 9a des Strafregistergesetzes 1968, BGBl. Nr. 277/1968, sowie die Abfrage und Verarbeitung von Vorwürfen nach Art. 56a der Richtlinie 2005/36/EG im Binnenmarkt-Informationssystem (IMI) vorgesehen.

§ 1a Abs. 1 bis 3, § 84, § 101 Abs. 1 und 2, § 102 und § 105 Abs. 5 PG 1965, § 1a Abs. 1 bis 3, § 21 Abs. 1 und 2 und § 21a Abs. 1 bis 3 BThPG und § 1a Abs. 1 bis 3, § 68 Abs. 1 und 2 und § 69 BB-PG ermächtigen die zuständigen Stellen, personenbezogene Daten und personenbezogene Daten besonderer Kategorien zum Zwecke der Ermittlung der Pensionshöhen zu erheben und zu verarbeiten.

BEWERTUNG

der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge

Die Notwendigkeit der Verarbeitung, Übermittlung oder Weiterverarbeitung personenbezogener Daten und personenbezogener Daten besonderer Kategorien ergibt sich für § 280 BDG 1979 aus dem jeweiligen in § 280 Abs. 1 BDG 1979 angeführten Rechtsverhältnis im Zusammenhang mit dem jeweiligen Zweck. Für die Praxis bedeutet dies, dass beispielsweise die zum Zwecke der Auszahlung gebührender Bezüge oder Pensionen erforderlichen personenbezogenen Daten oder personenbezogenen Daten besonderer Kategorien verarbeitet, übermittelt und weiterverarbeitet werden dürfen, um dieser rechtlichen Verpflichtung, die sich in diesem Fall aus einer Vorschrift gemäß § 280 Abs. 2 Z 2 BDG 1979 ergibt, nachzukommen.

Weiters ergibt sich die Notwendigkeit der beschriebenen Verarbeitungs-, Übermittlungs- und Weiterverarbeitungsvorgänge ebenfalls aus dem wichtigen öffentlichen Interesse an der Erfüllung der Kernaufgaben des Staates, an der Aufrechterhaltung und dem ordnungsgemäßen Funktionieren des Öffentlichen Dienstes und an einem rechtskonformen Vollzug insbesondere der in § 280 Abs. 2 BDG 1979 genannten Vorschriften, der beispielsweise ohne eine zeit- und ortsunabhängige Verfügbarkeit der jeweiligen Daten in der jetzigen Form nicht möglich wäre. Auch die Regelung der Nutzung der IKT-Infrastruktur zur Gewährleistung ihrer korrekten Funktionsfähigkeit sowie entsprechende Kontrollmöglichkeiten sind in diesem Zusammenhang in verhältnismäßigem Umfang notwendig und sachgerecht und bedingen in gewissem Ausmaß die Verarbeitung personenbezogener Daten oder personenbezogener Daten besonderer Kategorien.

Die Verarbeitung, Übermittlung und Weiterverarbeitung der jeweiligen personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien liegt aber auch im Interesse der betroffenen Personen und ist erforderlich, damit die Verantwortlichen oder die betroffenen Personen ihre Rechte und Pflichten ausüben oder geltend machen können.

Im Zusammenhang mit der Verarbeitung, Übermittlung und Weiterverarbeitung personenbezogener Daten besonderer Kategorien darf insbesondere auf Art. 9 Abs. 2 lit. b, g, h und j DSGVO verwiesen werden. Bezüglich Art. 9 Abs. 2 lit. h DSGVO in Verbindung mit Art. 9 Abs. 3 DSGVO wird auf die Regelungen zur Amtsverschwiegenheit sowie auf anderweitige Verschwiegenheitspflichten verwiesen (vgl. Art. 20 B-VG, § 46 BDG 1979, § 25 Abs. 6 Bundes-Gleichbehandlungsgesetz – B-GlBG, BGBl. Nr. 100/1993, § 54 Ärztegesetz 1998 – ÄrzteG 1998, BGBl. I Nr. 169/1998, ...).

An den Verarbeitungen, Übermittlungen und Weiterverarbeitungen gemäß § 280 Abs. 3 und 5 bis 7 BDG 1979 sowie § 280a Abs. 1, 6 und 7 BDG 1979 besteht ein allgemeines wichtiges öffentliches Interesse aufgrund der der oder dem Ermächtigten zukommenden Funktion.

Grundsätzlich bestehen Risiken, allerdings ist deren Eintritt einerseits nicht sehr wahrscheinlich und sind andererseits zahlreiche, wirksame und auf den jeweiligen Einzelfall bezogene Abhilfemaßnahmen vorgesehen, sodass die Datenschutz-Folgenabschätzung klar positiv ausfällt.

RISIKEN

Risiken, die bei der Verarbeitung und Übermittlung von personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien bestehen, werden insbesondere durch die strikte Einhaltung der Erfassungs- und Bearbeitungsvorgaben (z.B. Handbücher, Sicherheitskonzepte, Verfahrensvorschriften,...) in den diversen Anwenderapplikationen des Personalverfahrens und der Personalabrechnungen, bei der Pensionsbemessung und Pensionsauszahlung sowie beim Personalvollzug ohne IT-Unterstützung minimiert. Eine solche Minimierung der Risiken erfolgt standardmäßig in den IKT-Lösungen und IT-Verfahren für das IT-Personalmanagement des Bundes.

Als Risiken werden insbesondere in Erwägungsgrund 85 der DSGVO unter anderem genannt:

– „*physische, materielle oder immaterielle Schäden*“, „*unbefugte Aufhebung der Pseudonymisierung*“, „*Rufschädigung*“, „*Identitätsdiebstahl oder -betrug*“, „*finanzielle Verluste*“, „*Verlust der Vertraulichkeit bei Berufsgeheimnissen*“ oder „*erhebliche wirtschaftliche oder gesellschaftliche Nachteile*“:

Diese Risiken beziehungsweise Nachteile sind nahezu ausgeschlossen, weil mit den Strafbestimmungen des vierten bis sechsten sowie zweiundzwanzigsten Abschnittes des Besonderen Teiles des Strafgesetzbuches – StGB, BGBl. Nr. 60/1974, sowie den allenfalls anzuwendenden dienstrechtlichen Bestimmungen, wie beispielsweise dem Disziplinarrecht, wirksame Vorkehrungen gegen die unrechtmäßige Verarbeitung von Daten und somit das Entstehen von physischen, materiellen oder immateriellen Schäden bestehen. Wer die jeweiligen Daten missbraucht, geht angesichts der gerichtlichen Strafdrohung selbst ein sehr hohes Risiko ein.

Auf die Regelungen zur Amtverschwiegenheit sowie auf anderweitige Verschwiegenheitspflichten darf verwiesen werden (vgl. Art. 20 B-VG, § 46 BDG 1979, § 26 PVG, § 25 Abs. 6 B-GlBG...). Insbesondere finanzielle Verluste sind trotz der Verwendung von Finanzdaten aufgrund der durchgehenden Protokollierung von Verarbeitungen, Übermittlungen und Weiterverarbeitungen und der Kontrollmöglichkeit der Daten durch die betroffenen Personen nicht zu erwarten.

Eine unbefugte Aufhebung einer Pseudonymisierung ist bei schon jetzt umgesetzten Rollenkonzepten ausgeschlossen.

– „*Verlust der Kontrolle über personenbezogene Daten*“:

Diese Risiken werden dadurch verringert, dass Art. 5 Abs. 2 DSGVO als unmittelbar anwendbaren Grundsatz die Rechenschaftspflicht vorsieht. Die oder der Verantwortliche ist also nicht nur für die Einhaltung des Art. 5 Abs. 1 DSGVO verantwortlich, sondern muss auch dessen Einhaltung nachweisen können, was einzelfallbezogen durch entsprechende Protokollierungen sowie Dokumentation erfolgt. Im PM-SAP beispielsweise besteht auch derzeit bereits ein zentrales Protokollierungssystem, das jede Verarbeitung der Daten lückenlos protokolliert beziehungsweise durch ein definiertes Rollenkonzept nicht jede Person die Daten verarbeiten lässt.

Beispiele für Regelungen, die das Schriftlichkeitserfordernis bei der Dokumentation vorsehen, sind etwa § 79f Abs. 3 sowie § 79g Abs. 4 und 7 BDG 1979.

Diese Risiken werden auch dadurch weiter verringert, dass beispielsweise Strafregisterauskünfte nach ihrer Überprüfung unverzüglich zu löschen sind und dem Grundsatz der Rechenschaftspflicht folgend lediglich die jeweilige Verarbeitung protokolliert bleibt (vgl. § 204 Abs. 8 BDG 1979, § 3 Abs. 5 VBG, § 3 Abs. 1 RStDG, § 6 Abs. 5 LDG 1984, § 6 Abs. 5 LLDG 1985 und § 2 Abs. 3a RPG).

– „*Diskriminierung*“:

Dieses Risiko ist durch diverse Diskriminierungsverbote ausgeschlossen, insbesondere durch solche des B-GlBG oder etwa durch § 43a BDG 1979. Außerdem besteht für die betroffenen Personen in vielen Fällen die Ausübung des Rechtes auf Einsicht mittels ESS, wodurch zusätzlich eine Diskriminierung ausgeschlossen ist.

– „*Einschränkung der Rechte der betroffenen Personen*“:

Die Rechte der betroffenen Personen werden in § 280 Abs. 3 BDG 1979 vom Zeitpunkt des Einlangens eines Ersuchens einer zuständigen Behörde bis zum Zeitpunkt der Information der zuständigen Behörde an die Leiterin oder den Leiter der jeweiligen Zentralstelle beschränkt. Diese Möglichkeit ergibt sich aus Art. 23 DSGVO und erfolgt als bloße Verarbeitung aufgrund des Ersuchens der zuständigen Behörde zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Die Beschränkung der Rechte der betroffenen Person im notwendigen und verhältnismäßigen Ausmaß liegt im allgemeinen öffentlichen Interesse und stellt sicher, dass die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit gewährleistet ist. Die zuständige Behörde

soll durch die Vornahme der erforderlichen bloßen Verarbeitung durch die Leiterin oder den Leiter der jeweiligen Zentralstelle unterstützt werden.

Die Rechte der betroffenen Personen werden auch in § 280 Abs. 6 dritter Satz BDG 1979 beschränkt. Dies erfolgt jeweils im Rahmen der Öffnungsklausel des Art. 89 Abs. 2 DSGVO. Danach können die in den Art. 15, 16, 18 und 21 DSGVO angeführten Rechte der betroffenen Personen beschränkt werden. Dies erfolgt im Rahmen einer Abwägung, bei der überprüft werden muss, ob diese Rechte voraussichtlich die Verwirklichung der Forschungszwecke oder der statistischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungszwecke oder der statistischen Zwecke notwendig ist. Dadurch soll insbesondere sichergestellt werden, dass die für die wissenschaftlichen oder historischen Forschungszwecke oder die statistischen Zwecke notwendige Vollständigkeit der Daten gewährleistet und nicht durch Ausübung der genannten Rechte der betroffenen Personen ernsthaft beeinträchtigt oder unmöglich gemacht wird.

In § 280b Abs. 5 bis 8 BDG 1979 wird von der in Art. 23 DSGVO eröffneten Möglichkeit der Beschränkung der Pflichten und Rechte gemäß Art. 5, 12 bis 22 und 34 DSGVO Gebrauch gemacht. Dies erfolgt unter Beachtung des Wesensgehalts der Grundrechte und Grundfreiheiten und stellt eine notwendige und verhältnismäßige Maßnahme dar. Derartige Beschränkungen von Rechten und Pflichten müssen darüber hinaus der Sicherstellung bestimmter Zwecke dienen, unter denen beispielsweise in Art. 23 Abs. 1 lit. e DSGVO der „Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit“ genannt wird. Daneben können sich solche Beschränkungen beispielsweise auch auf Art. 23 Abs. 1 lit. h bis j DSGVO stützen. Die Verarbeitung, Übermittlung und Weiterverarbeitung von personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien ist für den Öffentlichen Dienst unerlässlich und liegt aufgrund des überwiegenden, berechtigten öffentlichen Interesses an der Aufrechterhaltung und dem ordnungsgemäßen und rechtskonformen Funktionieren des Öffentlichen Dienstes, insbesondere im Sinne einer Erfüllung der Kernaufgaben des Staates unter Wahrung der Grundsätze der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit, selbst im öffentlichen Interesse. Insbesondere ist es erforderlich, dass im Öffentlichen Dienst weiterhin die Möglichkeit zur Dienstaufsicht sowie zur Planstellenbewirtschaftung besteht und dass die Revisionsicherheit gewährleistet ist. Es ist daher erforderlich und sachgerecht, gewisse Beschränkungen der Rechte der betroffenen Personen vorzunehmen.

§ 280b Abs. 5 BDG 1979 schließt das Recht auf Berichtigung gemäß Art. 16 DSGVO bei unrichtigen oder unvollständigen personenbezogenen Daten oder personenbezogenen Daten besonderer Kategorien aus, wenn einer solchen Berichtigung die Rechtskraft oder die Verjährung entgegenstehen, oder wenn ein zumutbarer Rechtsweg besteht oder bestand. Damit ist klargestellt, dass das Recht auf Berichtigung auch im Anwendungsbereich der §§ 280 ff BDG 1979 nicht der Umgehung anderer rechtlicher Vorschriften dient.

§ 280b Abs. 6 BDG 1979 schließt das Recht auf Löschung gemäß Art. 17 DSGVO für Zeiten einer durch Gesetz oder Verordnung vorgesehenen Aufbewahrungspflicht oder Archivierung aus. Eine solche Möglichkeit besteht gemäß Art. 17 Abs. 3 DSGVO zur Erfüllung einer rechtlichen Verpflichtung, wie beispielsweise einer Aufbewahrungspflicht, die die Verarbeitung nach dem Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Zur Aufrechterhaltung des Öffentlichen Dienstes und der öffentlichen Ordnung und Sicherheit als allgemeines öffentliches Interesse und zur Sicherstellung der mit der Verarbeitung, Übermittlung und Weiterverarbeitung personenbezogener Daten und personenbezogener Daten besonderer Kategorien von betroffenen Personen verbundenen Kontroll-, Überwachungs- und Ordnungsfunktion ist die gesetzlich vorgesehene Verarbeitung, Übermittlung und Weiterverarbeitung der genannten Daten bis zum Ablauf der durch Gesetz oder durch Verordnung bestimmten Frist der Aufbewahrungspflicht erforderlich. Auf Art. 17 Abs. 3 lit. d und e DSGVO wird außerdem hingewiesen.

§ 280b Abs. 7 BDG 1979 regelt eine erforderliche und sachgerechte Beschränkung des Rechtes auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO. Die Überprüfung der Richtigkeit der personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien der betroffenen Person soll nämlich nicht dazu führen, dass in den standardisierten IKT-Lösungen und IT-Verfahren für das Personalmanagement des Bundes die Verarbeitung, Übermittlung und Weiterverarbeitung einzuschränken wäre, was beispielsweise ein momentanes Anhalten der Vorrückung oder eine nicht zeitgerechte Anweisung des zustehenden Bezuges zur Folge haben kann. Alleine das Bestehen dieser möglichen Folgen aufgrund der integrierten Systeme würde neben der Verursachung eines beträchtlichen

Verwaltungsaufwandes für viele betroffene Personen die Geltendmachung ihrer Rechte gemäß DSGVO erschweren oder faktisch unmöglich machen, weswegen für den Anwendungsbereich der §§ 280 ff BDG 1979 eine Beschränkung des Rechtes auf Einschränkung der Verarbeitung im erforderlichen Ausmaß vorgesehen ist. Gleiches gilt für den Zeitraum, in dem die betroffene Person ihr Recht auf Widerspruch geltend gemacht hat und noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen. Eine Beschränkung des Rechtes auf Einschränkung der Verarbeitung ist auch im Lichte des wichtigen wirtschaftlichen und finanziellen Interesses des Staates, beispielsweise im Haushalts- und Steuerbereich, erforderlich und sachgerecht im Sinne des Art. 23 Abs. 1 DSGVO, da etwa die rechtskonforme Abführung von Beiträgen zur Sozialversicherung und der Lohnsteuer ein wichtiges Ziel des allgemeinen öffentlichen Interesses darstellt, dessen Schutz die Beschränkung von Rechten rechtfertigt.

Aufgrund des überwiegenden, berechtigten öffentlichen Interesses an der Verarbeitung der personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien der Personen gemäß § 280 Abs. 1 BDG 1979 ist es erforderlich und sachgerecht, das Recht auf Widerspruch gemäß Art. 21 DSGVO in § 280b Abs. 8 BDG 1979 für Zeiten einer durch Gesetz oder Verordnung vorgesehenen Aufbewahrungspflicht oder Archivierung auszuschließen. Die Erforderlichkeit und Sachlichkeit dieser Beschränkung ergibt sich ebenfalls aus dem überwiegenden, berechtigten öffentlichen Interesse an der Aufrechterhaltung und dem ordnungsgemäßen Funktionieren des Öffentlichen Dienstes, konkret dem rechtskonformen Vollzug der Personaladministration und dem rechtskonformen Abführen von Beiträgen, beispielsweise zur Sozialversicherung und der Lohnsteuer. Verarbeitungen, Übermittlungen und Weiterverarbeitungen gemäß § 280 Abs. 1 BDG 1979 erfolgen ausschließlich zu in § 280 Abs. 2 BDG 1979 genannten Zwecken, sofern dies erforderlich ist. Auch für die weiteren Verarbeitungen, Übermittlungen und Weiterverarbeitungen gemäß den §§ 280 und 280a Abs. 1 und 7 BDG 1979 besteht ein überwiegendes, berechtigtes öffentliches Interesse, wobei auch auf Art. 21 Abs. 6 DSGVO hingewiesen wird. Darüber hinaus würde für den Fall, dass eine betroffene Person ihr Recht auf Widerspruch geltend macht, eine weitere Verarbeitung, Übermittlung und Weiterverarbeitung erforderlich werden, was dem grundsätzlichen Anliegen der betroffenen Person zuwiderlaufen würde. Es wird daher eine sachgerechte und erforderliche Beschränkung des Rechtes auf Widerspruch gemäß Art. 21 DSGVO im Sinne des Art. 23 DSGVO für Zeiten einer durch Gesetz oder Verordnung vorgesehenen Aufbewahrungspflicht oder Archivierung vorgesehen.

Die genannten Risiken sind nach Erwägungsgrund 75 DSGVO mit Eintrittswahrscheinlichkeit und Schwere anzugeben. Angesichts der verschwindend geringen Zahl von zwei Verurteilungen nach § 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem) im Jahr 2016 (Statistik Austria, Gerichtliche Kriminalstatistik 2016, https://www.statistik.at/web_de/statistiken/menschen_und_gesellschaft/soziales/kriminalitaet/index.html, [08.02.2018]) sowie einer Zahl von ca. 3,6 Mio. aktiven IT-Systemen in Österreich, ergibt sich eine Wahrscheinlichkeit von unter 1:1 Million, dass sich die von der DSGVO angeführten Risiken oder Nachteile verwirklichen. Die Zahl von 3 610 602 aktiven IT-Systemen ergibt sich aus der Zahl der Privathaushalte, die für das Jahr 2016 mit 3 865 000 beziffert wird (Statistik Austria, Haushaltsstatistik 2016, https://www.statistik.at/web_de/statistiken/menschen_und_gesellschaft/bevoelkerung/haushalte_familien_lebensformen/index.html, [08.02.2018]), der Zahl der Unternehmen, die für das Jahr 2015 mit 328 638 beziffert wird (Statistik Austria, Leistungs- und Strukturstatistik 2015, http://www.statistik.at/web_de/statistiken/wirtschaft/unternehmen_arbeitsstaetten/index.html, [08.02.2018]) sowie dem Faktor der IKT-Nutzung der für das Jahr 2016 für private Haushalte mit 85 Prozent und für Unternehmen mit 99 Prozent (Statistik Austria, IKT-Einsatz in Haushalten beziehungsweise Unternehmen, https://www.statistik.at/web_de/statistiken/energie_umwelt_innovation_mobilitaet/informationsgesellschaft/index.html, [08.02.2018]) beziffert wird.

Im Jahr 2016 (Statistik Austria, Gerichtliche Kriminalstatistik 2016, https://www.statistik.at/web_de/statistiken/menschen_und_gesellschaft/soziales/kriminalitaet/index.html, [08.02.2018]) erfolgten 57 Verurteilungen nach § 302 StGB (Missbrauch der Amtsgewalt). Wie viele der Verurteilungen etwa aufgrund des gezielten Beschaffens personenbezogener Daten oder personenbezogener Daten besonderer Kategorien durch Abfrage in für die Erfüllung dienstlicher Aufgaben eingerichteter Datenbanken oder aufgrund des Ermitteln personenbezogener Daten oder personenbezogener Daten besonderer Kategorien ohne dienstliche Rechtfertigung erfolgten, war nicht feststellbar. Daher kann für die Fälle des Missbrauches der Amtsgewalt keine Wahrscheinlichkeit des Verwirklichens der von der DSGVO angeführten Risiken oder Nachteile angegeben werden.

ABHILFEMAßNAHMEN

Die Datensicherheitsprozesse im IT-Personalmanagement orientieren sich an folgenden Normen, Standards und Empfehlungen:

- ISO 27001, ISO 27002 und ISO 27005 (Informationssicherheit);
- ISO 29100, ISO 29134 und ISO 29151 (Datenschutz);
- ÖNORM S 2109 und DIN 66399-1 (Akten- und Datenvernichtung);
- IT-Grundschutzkataloge (Gefährdungskataloge) des deutschen Bundesamts für Sicherheit in der Informationstechnik;
- Datenschutz-Leitlinien der österreichischen Datenschutzbehörde;
- Datenschutz-Leitlinien der Artikel-29-Datenschutzgruppe.

Darüber hinaus werden insb. folgende E-Government Konventionen berücksichtigt:

- BLSG-Konvention „Portalverbund – Grundschutz“
- BLSG-Konvention „Portalverbund – Sicherheitsmaßnahmen“
- BLSG-Konvention „Portalverbund – Verwaltungsprozess für zentrale Dienste“
- BLSG-Konvention „Portalverbundprotokoll Version 2“
- BLSG-Konvention „Sicherheitsklassen – Zugriff von Benutzern auf Anwendungen“
- BLSG-Konvention „Revisionsabfrage im Portalverbund“
- BLSG-Konvention „Datensicherheitsmaßnahmen für Webanwendungen“
- BLSG-Konvention „Common Audit Trail Exchange Format“
- BLSG-Konvention „Sicherheitsstufen – Kommunikation Bürger – Behörde“
- ISK-Vorgabe „Nationale Kryptostrategie“
- ISK-Vorgabe „TLS-Vorgaben für klassifizierte Informationen“
- ISK-Vorgabe „Vorgaben zu E-Mail für klassifizierte Informationen“

Als Maßnahmen, Garantien und Verfahren zur Eindämmung von Risiken werden insbesondere in Erwägungsgrund 78 der DSGVO unter anderem genannt:

– „*Minimierung der Verarbeitung personenbezogener Daten*“ und „*Verwendungsbeschränkung*“:

Die Minimierung der Verarbeitung personenbezogener Daten ergibt sich unmittelbar aus Art. 5 Abs. 1 lit. c DSGVO. Dort wird die Datenminimierung in dem Sinne geregelt, dass Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen. Dieser Grundsatz ist in vielfältiger Weise auch im Gesetzestext anzutreffen, insbesondere durch den konsequenten Einsatz des Kriteriums der Erforderlichkeit der jeweiligen Verarbeitung, Übermittlung oder Weiterverarbeitung (vgl. § 280 BDG 1979). Aus dem Kriterium der Erforderlichkeit ist ebenso die Beachtung des Grundsatzes der Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e DSGVO abzuleiten, wonach personenbezogene Daten in einer Form gespeichert werden müssen, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Der sich aus Art. 5 Abs. 1 lit. b DSGVO ergebende Grundsatz der Zweckbindung ist ebenso durchgehend umgesetzt (vgl. § 280 BDG 1979). Danach dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Eine Weiterverarbeitung zu einem anderen Zweck, der ebenso wie der ursprüngliche Zweck der Verarbeitung durch § 280 Abs. 2 BDG 1979 erfasst sein muss, ist daher nur möglich, sofern die personenbezogenen Daten oder die personenbezogenen Daten besonderer Kategorien zu diesem „neuen“ Zweck ebenfalls erhoben und verarbeitet werden dürften, eine derartige neuerliche Erhebung bereits vorhandener Daten jedoch aus Gründen der Verwaltungsvereinfachung sowie den Grundsätzen der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit folgend unterbleibt, sofern eine Weiterverarbeitung erfolgen kann und darf.

Dabei gilt eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Art. 89 Abs. 1 DSGVO nicht als unvereinbar mit den ursprünglichen Zwecken. Die rechtmäßige Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, ist auf Grundlage des § 280 BDG 1979 zulässig, sofern dies erforderlich ist. Die Erforderlichkeit in diesem Zusammenhang ergibt sich aus der Zusammenschau mit den in Art. 23 Abs. 1 DSGVO genannten Zielen, für die die Verarbeitung eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz dieser Ziele darstellen muss. Insbesondere ist hierbei an die öffentliche Sicherheit, die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen sowie an den Schutz sonstiger

wichtiger Ziele des allgemeinen öffentlichen Interesses eines Mitgliedstaates zu denken. Davon abgedeckt sind auch wichtige wirtschaftliche oder finanzielle Interessen des jeweiligen Mitgliedstaates. Insbesondere darf an dieser Stelle auch das wichtige öffentliche Interesse am Funktionieren des Öffentlichen Dienstes und an einem rechtskonformen Vollzug der gesetzlichen Vorschriften hervorgehoben werden.

Zu § 280 Abs. 1 und 2 BDG 1979 wird festgehalten, dass eine über die in diesen Absätzen festgelegten, eindeutigen und legitimen Zwecke hinausgehende Verarbeitung, Übermittlung und Weiterverarbeitung, sofern nicht ausdrücklich normiert, auf Grundlage des § 280 Abs. 1 und 2 BDG 1979 nicht vorgesehen ist. Von der Ermächtigung des § 280 Abs. 1 und 2 BDG 1979 sind lediglich erforderliche Übermittlungen zwischen den Leiterinnen und Leitern der Zentralstellen erfasst. Darüber hinausgehende Übermittlungen an Leiterinnen oder Leiter der Zentralstellen oder Dritte bleiben von dieser Bestimmung unberührt und sind anhand ihrer jeweiligen Rechtsgrundlage zu beurteilen.

§ 280 Abs. 6 BDG 1979 beinhaltet etwa eine Regelungen zur unverzüglichen Auflösung des Personenbezuges bei der Verarbeitung von personenbezogenen Daten oder personenbezogenen Daten besonderer Kategorien zu statistischen Zwecken oder zu wissenschaftlichen oder historischen Forschungszwecken. Eine Minimierung der Verarbeitung findet daher in der Praxis jedenfalls dann statt, wenn eine Verarbeitung personenbezogener Daten für den beabsichtigten Zweck nicht erforderlich ist, also beispielsweise im Zusammenhang mit statistischen Auswertungen oder der Erstellung von Controllingberichten.

Gemäß § 79e Abs. 3 BDG 1979 dürfen etwa Inhalte übertragener Nachrichten nur dann im Sinne des § 79e BDG 1979 kontrolliert werden, wenn dies für die Erreichung der angeführten Zwecke unbedingt erforderlich ist. Weiters ist eine Abwägung vorzunehmen, die die erforderliche Verarbeitung sowie die Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten oder personenbezogener Daten besonderer Kategorien erfordern, berücksichtigt (vgl. § 79e Abs. 2 BDG 1979).

§ 79e Abs. 4 BDG 1979 sieht im Sinne des Grundsatzes der Datenminimierung vor, dass sich Kontrollmaßnahmen nur auf die unbedingt erforderliche Anzahl an Bediensteten beziehen dürfen.

§ 79f Abs. 5 BDG 1979 regelt beispielsweise ein Weiterverarbeitungsverbot für Daten im dort angeführten Sinn.

Gemäß § 10a PVG erfolgt beispielsweise eine Einsichtnahme grundsätzlich nur ins Personalverzeichnis und für darüber hinausgehende Verarbeitungen wird die Zustimmung der oder des betroffenen Bediensteten benötigt.

Eine weitere Umsetzung insbesondere des Grundsatzes der Datenminimierung findet sich beispielsweise in den jeweiligen gesetzlichen Bestimmungen, die vorsehen, dass Strafregisterauskünfte nach ihrer Überprüfung unverzüglich zu löschen sind (vgl. § 204 Abs. 8 BDG 1979, § 3 Abs. 5 VBG, § 3 Abs. 1 RStDG, § 6 Abs. 5 LDG 1984, § 6 Abs. 5 LLDG 1985 und § 2 Abs. 3a RPG).

§ 280a Abs. 2 bis 5 BDG 1979 enthält Bestimmungen zur Datenaufbewahrung. Bei Gemeinsam Verantwortlichen ist dem Grundsatz der Datenminimierung folgend die Aufbewahrungspflicht nur von einem Verantwortlichen wahrzunehmen. Gesetzlich ist eine fünfzehnjährige Frist für personenbezogene Daten und personenbezogene Daten besonderer Kategorien vorgesehen. Für Protokolldaten über lesende Zugriffe ist eine dreijährige Frist und für Protokolldaten über datenändernde Zugriffe eine siebenjährige Frist vorgesehen. § 280a Abs. 6 BDG 1979 bestimmt, dass eine durch Gesetz oder Verordnung vorgesehene längere Aufbewahrungspflicht oder Archivierung den in § 280 Abs. 2 bis 5 BDG 1979 vorgesehenen Aufbewahrungspflichten vorgeht. Etwaige längere Aufbewahrungspflichten sollen demnach nicht durch die Einführung einer Aufbewahrungspflicht gemäß § 280a BDG 1979 verkürzt werden. Ebenso unberührt bleiben soll die Löschpflicht von Strafregisterauskünften. Werden jedoch speziellere Fristen für Aufbewahrungspflichten durch den Verantwortlichen oder die gemeinsam Verantwortlichen mittels Verordnung vorgesehen, so gehen diese der jeweiligen Frist der Aufbewahrungspflicht gemäß § 280a Abs. 2 bis 5 BDG 1979 vor. Die Fristen für Protokolldaten über lesende Zugriffe müssen jedoch mindestens ein Jahr und für Protokolldaten über datenändernde Zugriffe mindestens drei Jahre betragen, damit insbesondere die Rechte betroffener Personen nicht durch zu kurze Fristen eingeschränkt werden. Eine durch Gesetz oder Verordnung vorgesehene längere Frist einer Aufbewahrungspflicht oder Archivierung geht gemäß § 280 Abs. 6 BDG 1979 auch einer durch Verordnung gemäß § 280a Abs. 7 BDG 1979 festgesetzten kürzeren Frist vor. Gemeinsam Verantwortliche haben beim Erlassen einer Verordnung gemäß § 280a Abs. 7 BDG 1979 das Einvernehmen herzustellen. Durch die Verordnungsermächtigung in § 280a Abs. 7 BDG 1979 soll insbesondere den Grundsätzen der Speicherbegrenzung und Datenminimierung besonders Rechnung getragen werden.

Die Zugriffs- und Berechtigungskonzepte des IT-Personalmanagements entsprechen dem Grundsatz der Beschränkung auf das notwendige Maß.

– „*schnellstmögliche Pseudonymisierung personenbezogener Daten*“ (siehe auch Erwägungsgrund 28 DSGVO):

Eine Pseudonymisierung der auf Grundlage des § 280 BDG 1979 erhobenen personenbezogenen Daten oder personenbezogenen Daten besonderer Kategorien selbst ist nicht möglich, weil im Sinne des jeweiligen Rechtsverhältnisses eine zweifelsfreie Zuordnung sowohl in der analogen, als auch in der digitalen Welt möglich bleiben muss, was auch dem Kriterium der Erforderlichkeit entspricht. Ist eine Auflösung des Personenbezuges durch geeignete technische Mittel (vgl. § 280 Abs. 6 BDG 1979) jedoch möglich, so wird diese insbesondere gemäß den Grundsätzen der Datenminimierung und der Speicherbegrenzung und im Sinne des Art. 32 DSGVO vorgenommen, sofern nicht ohnedies eine Löschung zu erfolgen hat.

– „*Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten*“ und „*Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Personen*“:

Durch die explizite gesetzliche Regelung der Datenverarbeitung sowie deren Zwecke wird den Anforderungen der Transparenz bereits durch die Kundmachung in hohem Maße Rechnung getragen.

Durch die Benennung einer oder eines jeweils zuständigen Datenschutzbeauftragten oder nötigenfalls auch mehrerer Datenschutzbeauftragter gemäß Art. 37 bis 39 DSGVO wird eine direkte Ansprechperson deklariert, der betroffene Personen unter Wahrung der Geheimhaltung und der Vertraulichkeit zu allen Angelegenheiten, die mit der Verarbeitung ihrer personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien oder mit der Wahrnehmung ihrer Rechte im Zusammenhang stehen, Fragen stellen können. So ist etwa eine betroffene Person, die ein gemäß § 280b Abs. 5 bis 8 BDG 1979 beschränktes Recht geltend macht, unter Hinweis darauf gemäß § 280b Abs. 4 BDG 1979 an die zuständige Datenschutzbeauftragte oder den zuständigen Datenschutzbeauftragten zu verweisen.

Außerdem wird durch das gemäß Art. 30 DSGVO zu führende Verzeichnis von Verarbeitungstätigkeiten, das der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen ist, dargestellt, welche Verarbeitungstätigkeiten jeweils vorgenommen werden und der jeweiligen Zuständigkeit unterliegen.

Beispiele für Informationspflichten im Zusammenhang mit betroffenen Personen finden sich etwa in § 79f und § 79g BDG 1979.

Über das Employee Self Serviceportal erfolgen entsprechende Informationen an die betroffenen Personen des IT-Personalmanagements.

– „*Datensicherheitsmaßnahmen*“ (Erwägungsgrund 83 DSGVO):

Durch entsprechende technische und personelle Maßnahmen wird im Einzelfall sichergestellt, dass personenbezogene Daten oder personenbezogene Daten besonderer Kategorien in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet und einen entsprechenden Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung bietet, wodurch vor allem dem Grundsatz der Integrität und Vertraulichkeit gemäß Art. 5 Abs. 1 lit. f DSGVO Rechnung getragen wird.

Die Verantwortlichen gemäß § 280 Abs. 1 und die gemeinsam Verantwortlichen gemäß § 280b Abs. 2 haben jeweils gemäß Art. 32 bis 34 DSGVO für die Sicherheit der personenbezogenen Daten, der personenbezogenen Daten besonderer Kategorien sowie der Protokolldaten zu sorgen. Die Bundeskanzlerin oder der Bundeskanzler ist gemäß § 280a Abs. 7 BDG 1979 ermächtigt, zum Zwecke der rechtskonformen Verfahrensgestaltung, der Fehlerbehebung sowie der Datensicherheit in den von ihr oder ihm bereitgestellten oder betriebenen IKT-Lösungen und IT-Verfahren für das Personalmanagement des Bundes erforderliche nicht datenändernde Verarbeitungen, Übermittlungen und Weiterverarbeitungen von personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien durchzuführen. Die Erforderlichkeit der Verarbeitung, Übermittlung und Weiterverarbeitung personenbezogener Daten und personenbezogener Daten besonderer Kategorien zu den genannten Zwecken ist eng auszulegen. Datensicherheit bezieht sich nicht nur auf den physischen Zugang zu den Personaldatensystemen, sondern bedeutet auch, dass sichergestellt wird, dass die IKT-Lösungen und IT-Verfahren für das Personalmanagement des Bundes Verarbeitungen, Übermittlungen und Weiterverarbeitungen von personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien nur berechtigten Personen ermöglichen und diese Daten nur berechtigten Personen zur Verfügung stehen. Personenbezogene Daten und personenbezogene Daten besonderer Kategorien sind vor unrechtmäßigen Verarbeitungen, Übermittlungen oder Weiterverarbeitungen zu schützen, was insbesondere durch entsprechende Protokollierung zu erfolgen hat. Daher ist von dem oder den jeweils Verantwortlichen sicherzustellen, dass bestehende Protokolldaten nicht verändert werden können.

Datensicherheitsmaßnahmen werden etwa auch durch Sicherheitsanalysen bei der Programmierung sowie bereits jetzt umgesetzte Rollenkonzepte und die damit eindeutige Identifikation der oder des jeweiligen Verarbeitenden getroffen.

Weiters trägt die Benennung einer oder eines jeweils zuständigen Datenschutzbeauftragten maßgeblich zur Datensicherheit bei. Hinzu kommen beispielsweise entsprechende Schulungen, Handbücher, Sicherheitskonzepte oder gegebenenfalls Weisungen, die auf den jeweiligen Einzelfall abstellen. Außerdem bestehen Verarbeitungs-, Übermittlungs- und Weiterverarbeitungsmöglichkeiten stets nur für Personen, die sich in ihrem jeweiligen Rechtsverhältnis entsprechend bewährt und als verlässlich erwiesen haben. Insbesondere die Bestimmungen zur Abwehr von Schäden an der IKT-Infrastruktur und zur Gewährleistung ihrer korrekten Funktionsfähigkeit und zu Kontrollmaßnahmen im Sinne des 5a. Unterabschnitts des BDG 1979 bewirken durch die dort gesetzten Maßnahmen ebenso eine Erhöhung der Datensicherheit.

Zu § 119a LDG 1984:

Die Ermächtigung für die Länder bestimmte Daten zu verarbeiten, bedarf einer Anpassung an die DSGVO.

Neben der Verarbeitung, Übermittlung und Weiterverarbeitung von Daten für Landeslehrpersonen gemäß § 1 LDG 1984 und Landesvertragslehrpersonen gemäß § 1 LVG erstreckt sich die gegenständliche Ermächtigung auch einerseits auf Daten von Bundeslehrpersonen gemäß § 1 Abs. 1 BDG 1979 sowie § 1 Abs. 1 VBG, um eine Verarbeitung von Daten von Bundeslehrpersonen, die an Pflichtschulen mitverwendet werden, sicherzustellen und andererseits auf in einem Dienstverhältnis zu einem privaten Rechtsträger stehende Lehrpersonen (Lehrpersonen nach § 19 Abs. 3 PrivSchG sowie kirchlich bestellte Religionslehrpersonen), da für die Lehrpersonen nach § 19 Abs. 3 PrivSchG die Besoldung durch die Länder erfolgen muss.

Im Übrigen wird auf die Ausführungen zu §§ 280, 280a und 280b BDG 1979 verwiesen, insoweit die jeweiligen Absätze in § 119a für anwendbar erklärt werden.

Zu § 119h und § 124a LLDG 1985:

Bezüglich § 119h wird, insoweit die jeweiligen Absätze in § 119h für anwendbar erklärt werden, auf die Ausführungen zu §§ 280, 280a und 280b BDG 1979 verwiesen.

Aufgrund der umfassenden Neuregelung der Datenverarbeitung in § 119h kann § 124a entfallen.