D A T E N S I C H E R H E I T S V O R S C H R I F T

F Ü R

Statistik Austria

INHALTSVERZEICHNIS

1 ALLGEMEINES 4
1.1 Gegenstand und Geltungsbereich 4
1.2 Gesetzliche Grundlagen und Sonderregelungen 4
1.3 Grundrecht auf Datenschutz 5
1.4 Datengeheimnis 5
1.5 Begriffsbestimmungen 6
2 AUFGABENVERTEILUNG 9
2.1 Auftraggeberin und Dienstleisterin 9
2.2 Anwender und Benutzer 9
2.3 Verantwortliche und Auftragsverarbeiter 10
3 VERARBEITUNGSTÄTIGKEITEN 11
4 INFORMATIONSVERPFLICHTUNGEN 12
5 RECHTE VON BETROFFENEN NATÜRLICHEN PERSONEN 14
6 AUFTRÄGE 15
7 BELEHRUNGSPFLICHT 16
8 ZUTRITTSBESCHRÄNKUNG 16
9 ZUGRIFFSBESCHRÄNKUNG 17
10 BETRIEBSBESCHRÄNKUNG 18
11 PROTOKOLLIERUNG 19
12 DATENSICHERUNG UND DATENAUSLAGERUNG 19
13 KONTROLLE 20
14 INKRAFTTRETEN 20

1 ALLGEMEINES

1.1 Gegenstand und Geltungsbereich

(1) Diese Datensicherheitsvorschrift gilt für die Mitarbeiterinnen und Mitarbeiter aller Organisationseinheiten der Bundesanstalt „Statistik Österreich“ (im Folgenden Statistik Austria), die vertrauliche und personenbezogene Daten automationsunterstützt oder in einem manuell geführten Dateisystem verarbeiten.

(2) Diese Datensicherheitsvorschrift regelt die Datensicherheitsmaßnahmen, die unter Bedachtnahme auf den Stand der technischen Möglichkeiten sowie auf die wirtschaftliche Vertretbarkeit sicherstellen, dass die Daten vor zufälliger oder unrechtsmäßiger Zerstörung und vor Verlust geschützt sind, dass die Verwendung vertraulicher und personenbezogener Daten ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zur Kenntnis gelangen.

(3) Die einzelnen Bestimmungen dieser Datensicherheitsvorschrift gelten für die Mitarbeiterinnen und Mitarbeiter aller Organisationseinheiten von Statistik Austria, soweit nicht strengere oder weitergehende Regelungen (z. B. Bestimmungen für die Nutzung einer IT-Anwendung) vorgeschrieben sind.

1.2 Gesetzliche Grundlagen und Sonderregelungen

(1) Die gegenständliche Datensicherheitsvorschrift wird gemäß der Datenschutz-Grundverordnung (DSGVO)[1] und dem Datenschutzgesetz (DSG)[2] idgF erlassen.

(2) Die Datensicherheitsvorschrift ist eine Dienstanweisung, deren Verletzung dienstrechtliche Konsequenzen nach sich zieht.

(3) Bei Gefahr in Verzug sowie auch zur Abwehr eines drohenden wirtschaftlichen Schadens kann jede Mitarbeiterin und jeder Mitarbeiter im Rahmen der ihr oder ihm zugewiesenen Aufgaben auch dem Anlassfall entsprechend, gerechtfertigte Maßnahmen ergreifen, die in der Datensicherheitsvorschrift nicht vorgesehen sind. Über solche Maßnahmen ist der Leitung von Statistik Austria sowie der oder dem von dieser bestellten Datenschutzbeauftragten unverzüglich zu berichten. Bei Gefahr im Verzug und Maßnahmen ohne Schädigungsabsicht haftet die Arbeitgeberin für allfällige durch solche Maßnahmen entstandene Schäden.

[1] 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 4.5.2016 S. 1

[2] Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), StF: BGBl. I Nr. 165/1999

1.3 Grundrecht auf Datenschutz

Das Grundrecht auf Datenschutz natürlicher Personen ist in Art. 8 der Europäischen Menschenrechtskonvention, Art. 7 und 8 der Charta der Grundrechte der Europäischen Union, Art. 16 des Vertrages über die Arbeitsweise der Europäischen Union, Art. 1 DSGVO und § 1 DSG verankert.

Art. 1 Abs. 2 DSGVO
Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

1.4 Datengeheimnis

§ 6 DSG
(1) Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).

(2) Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

(3) Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen.

(5) Ein zugunsten eines Verantwortlichen bestehendes gesetzliches Aussageverweigerungsrecht darf nicht durch die Inanspruchnahme eines für diesen tätigen Auftragsverarbeiters, insbesondere nicht durch die Sicherstellung oder Beschlagnahme von automationsunterstützt verarbeiteten Dokumenten, umgangen werden.

1.5 Begriffsbestimmungen

Begriffe der DSGVO (Begriffsbestimmungen Art. 4)

(1) Personenbezogene Daten:
Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(2) Verarbeitung:
Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(3) Pseudonymisierung:
Die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

(4) Dateisystem:
Jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.

(5) Verantwortlicher:
Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(6) Auftragsverarbeiter:

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(7) Empfänger:
Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

(8) Dritter:
Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

(9) Einwilligung der betroffenen Person:
Jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

(10) Verletzung des Schutzes personenbezogener Daten:
Eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Sonstige Begriffe

(11) Datenschutzbeauftragte/r:
Als Beauftragte für Datenschutz von Statistik Austria bestellte und in Ausübung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei gestellte Person, die gemäß Abschnitt 4 DSGVO und § 5 DSG die Aufgaben der Unterrichtung und Beratung, Überwachung der Einhaltung und Zusammenarbeit mit der Aufsichtsbehörde auf dem Gebiet des Datenschutzes wahrnimmt.

(12) Sensible Daten:
Personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person („besondere Kategorien personenbezogener Daten“ gemäß Art. 9 DSGVO); personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gelten per definitionem nicht als „besondere Kategorien personenbezogener Daten“ (Art. 9 DSGVO), sie unterliegen aber auch einem speziellen Schutz gemäß Art. 10 DSGVO.

(13) IT-Arbeitsmittel:
Alle IT-Endgeräte, Peripherie-Geräte, Datenträger sowie Software, die in der IT-Infrastruktur von Statistik Austria eingebunden sind. IT-Endgeräte sind z.B. Desktops, Notebooks, Tablets, Tablet-PCs, Smartphones; Peripherie Geräte sind z.B. Maus, Tastatur, Drucker, Scanner, Bildschirm, Hubs; Datenträger sind z.B. USB-Sticks, Speicherkarten aller Art, mobile Festplatten, Multimediageräte (Kameras, Mobiltelefon); Software sind z.B. Programme, Apps, Skripte, Makros, Tools, Treiber, Betriebssysteme.

(14) IT-Anwendung:
Durch den Einsatz von IT-Sachressourcen (Hardware und Software) automationsunterstützt ablaufendes Verfahren zur Bewältigung bestimmter Aufgaben.

(15) Individuelle Datenverarbeitung (IDV):
Jene Form der automationsunterstützten Datenverarbeitung, bei der am Arbeitsplatz mittels der dort verfügbaren Rechnerkapazität mit arbeitsplatzorientierten Anwender-Standardsoftwareprodukten (Softwarewerkzeugen) automationsunterstützte Verfahren eigenständig und damit eigenverantwortlich gestaltet oder genutzt werden.

(16) IDV-Anwendung:
IT-Anwendung im Rahmen der individuellen Datenverarbeitung.

(17) Server:
Rechner mit besonderen Leistungsmerkmalen, auf dem auch arbeitsplatzübergreifende Aufgaben abgewickelt werden können.

(18) Betriebsräume:
Räume, in denen Datenendgeräte betrieben werden.

(19) Rechnerräume:
Räume, in denen Großrechner und/oder Server betrieben werden.

(20) Auftraggeberin:
Hausinterne Stelle, die über die Verarbeitung von personenbezogenen Daten entscheidet.

(21) Dienstleisterin:
Hausinterne Stelle, die personenbezogene Daten im Auftrag der Auftraggeberin verarbeitet.

2 AUFGABENVERTEILUNG

Die Aufgaben und die zu deren Erfüllung vorgesehenen Kompetenzen der Organisationseinheiten sind durch das Organisationsmanagement und die Personalzuordnung in der jeweils aktuellen Fassung festgelegt. Diese Regelungen bilden in jedem Fall die Grundlage für die Aufgabenverteilung im Sinne dieser Vorschrift.

2.1 Auftraggeberin und Dienstleisterin

(1) Auftraggeberin für eine IT-Anwendung ist die Leitung einer Organisationseinheit bzw. die Projektleitung (nach Abstimmung mit der Leitung von Statistik Austria). Die IT-Abteilung nimmt, sofern sie nicht selbst als Auftraggeberin eigenständig über die Verarbeitung von personenbezogenen Daten entscheidet, ihre Aufgaben als Dienstleisterin für die jeweilige Leitung einer Organisationseinheit bzw. die Projektleitung wahr.

(2) Die Auftraggeberin legt nachweislich die Verantwortlichkeiten betreffend die Durchführung von Betroffenenrechten fest.

2.2 Anwender und Benutzer

(1) Als Anwender gelten jene Bedienstete, die eine IT-Anwendung eigenständig und damit eigenverantwortlich gestalten und nutzen (z. B. IDV-Anwender).

(2) Benutzer sind jene Bedienstete, die eine IT-Anwendung ohne eigene Gestaltungsmöglichkeit lediglich auftragsgemäß nutzen (z. B. Benutzer einer zentral von der IT-Abteilung erstellten bzw. zur Verfügung gestellten IT-Anwendung).

2.3 Verantwortliche und Auftragsverarbeiter

(1) Statistik Austria kann als Verantwortliche eigener Datenanwendungen oder als Auftragsverarbeiterin im Auftrag eines anderen Verantwortlichen tätig werden.

(2) Liegt bei einer Datenverarbeitung personenbezogener Daten eine gemeinsame Verantwortlichkeit mit einem oder mehreren anderen Verantwortlichen vor, so legt Statistik Austria mit dem/den gemeinsam Verantwortlichen in einer Vereinbarung in transparenter Form fest, wer welche Verpflichtung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 DSGVO nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht gesetzlich festgelegt sind.

(3) Auftragsverarbeiter dürfen nur unter Einhaltung der Bestimmungen des Artikels 28 DSGVO in Anspruch genommen werden. Vor Heranziehung von Auftragsverarbeitern ist die Zustimmung der Leitung von Statistik Austria einzuholen. Die Verarbeitung darf nur auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments, der bzw. das die Auftragsverarbeiterin bzw. den Auftragsverarbeiter in Bezug auf Statistik Austria bindet, erfolgen, und in denen Gegenstand, Dauer, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen und Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Weiters hat die Auftragsverarbeiterin bzw. der Auftragsverarbeiter die personenbezogenen Daten nur auf dokumentierte Weisung von Statistik Austria zu verarbeiten; alle zur Sicherheit der Daten erforderlichen Maßnahmen zu ergreifen; die Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einzuhalten; angesichts der Art der Verarbeitung Statistik Austria nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, ihrer Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechte nachzukommen und unter Berücksichtigung der Art der Verarbeitung und der zur Verfügung stehenden Informationen Statistik Austria bei der Einhaltung der datenschutzrechtlichen Pflichten zu unterstützen; nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl von Statistik Austria zu löschen oder zurückzugeben, sofern nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht; Statistik Austria alle erforderlichen Informationen zum Nachweis der Einhaltung der niedergelegten Pflichten zur Verfügung zu stellen und Überprüfungen — einschließlich Inspektionen –, die von Statistik Austria oder einem von ihr beauftragten Prüfer durchgeführt werden, zu ermöglichen und dazu beizutragen.

3 VERARBEITUNGSTÄTIGKEITEN

(1) Die Verarbeitung von Daten darf nur in dem Umfang und für die Zeitdauer erfolgen, wie sie in den Rechtsvorschriften, Verträgen und Zustimmungserklärungen ihre rechtliche Deckung finden. Jede Auftraggeberin dokumentiert die Verarbeitungstätigkeiten personenbezogener Daten, die ihrer Zuständigkeit unterliegen, anhand eines vorgegebenen Datenverarbeitungsformulars, das die in Artikel 30 DSGVO aufgelisteten Angaben [Name und Kontaktdaten von Statistik Austria; ggf. des gemeinsam mit ihr Verantwortlichen; Kontaktdaten der/ des Datenschutzbeauftragte/n; Zwecke der Verarbeitung; betroffene Personenkreise und Datenarten; Kategorien von Empfängern (einschließlich Empfänger in Drittländern oder internationalen Organisationen); wenn möglich: Löschungsfristen; Beschreibung technischer und organisatorischer Maßnahmen] umfasst. Die Datenverarbeitungsformulare zu den einzelnen Datenverarbeitungen werden zentral in einem Verzeichnis aller Verarbeitungstätigkeiten personenbezogener Daten von Statistik Austria zusammengeführt und sind der Datenschutzbehörde auf Anfrage zur Verfügung zu stellen. Auch Auftragsverarbeiter müssen schriftlich ein Verzeichnis aller Kategorien von im Auftrag der/des Verantwortlichen durchgeführten Tätigkeiten führen.

(2) Die Auftraggeberin sorgt dafür, dass personenbezogene Daten nach Ablauf der zulässigen Aufbewahrungsfristen gelöscht werden.

(3) Beruht die Verarbeitung auf der Einwilligung einer betroffenen Person, muss die Auftraggeberin nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

(4) Die Auftraggeberin trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung –, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen. Sie trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass grundsätz-

lich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

(5) Die in der Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV) angeführten Datenverarbeitungen personenbezogener Daten sind von der Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 1 und 5 DSGVO ausgenommen.

(6) Es ist sicherzustellen, dass die Informationen von Statistik Austria entsprechend ihren Sicherheitserfordernissen geschützt werden. Dazu wurde eine Informationsklassifizierung der Statistik Austria in Datenklassen erstellt, Schutzziele zum Erreichen bzw. Einhalten der Informationssicherheit und je nach Schutzbedarf der Informationen geeignete Schutzniveaus zum Schutz der Daten definiert. Alle vorhandenen Datenkategorien sind aufgrund einer Risikobewertung den definierten Datenklassen und den jeweiligen Schutzniveaus in den Sicherheitsdimensionen zugeordnet. Daraus resultieren Auswirkungsniveaus und entsprechende Sicherheitsklassen. Jede Auftraggeberin ordnet die Datenbestände ihres Zuständigkeitsbereiches der aktuellen Informationsklassifizierung zu.

(7) Die Nutzung der IT-Infrastruktur und die damit verbundenen IT-Sicherheitsvorkehrungen von Statistik Austria sind in der jeweils aktuell geltenden Richtlinie zur IT-Nutzung verbindlich geregelt und vorgegeben.

(8) Für die statistische Geheimhaltung in Publikationen und Weitergabe von Daten ist die Richtlinie „Statistische Geheimhaltung in Publikationen und bei Weitergabe von Daten“ einzuhalten.

4 INFORMATIONSVERPFLICHTUNGEN

(1) Werden personenbezogene Daten direkt bei den betroffenen Personen erhoben, teilt jede Auftraggeberin den betroffenen Personen die Informationen, die in Artikel 13 DSGVO vorgegeben sind, mit. Die Informationen umfassen den Namen und die Kontaktdaten von Statistik Austria; die Kontaktdaten der/des Datenschutzbeauftragte/n; die Zwecke der Verarbeitung und deren Rechtsgrundlage; ggf. die Kategorien von Empfängern (einschließlich Empfänger in Drittländern oder internationalen Organisationen); die Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer; das Bestehen von Betroffenenrechten (vgl. dazu **Punkt 5**); wenn die Verarbeitung auf Einwilligung beruht, das Bestehen des Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird; das Bestehen eines Beschwerderechts bei der Datenschutzbehörde; ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist; ob die betroffene

Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte. Eine Ausnahme von der Informationspflicht besteht nur dann, wenn die betroffenen Personen bereits über diese Informationen verfügen. Entsprechend dem Grundsatz der Zweckbindung, stellt die Auftraggeberin für den Fall, dass sie beabsichtigt, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, der betroffenen Person Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen zur Verfügung. Eine Weiterverarbeitung für ausschließlich statistische Zwecke unter den Bedingungen des § 7 DSG und den gesetzlichen Vorgaben des Bundesstatistikgesetzes gilt dabei als vereinbar mit dem ursprünglichen Zweck und widerspricht nicht der ursprünglichen Zweckbindung.

(2) Werden personenbezogene Daten nicht bei den betroffenen Personen selbst erhoben, teilt jede Auftraggeberin den betroffenen Personen die Informationen, die in Artikel 14 DSGVO vorgegeben sind, mit. Dies kann unterbleiben, wenn die betroffenen Personen über die Informationen bereits verfügen, die Erteilung der Information unmöglich oder mit unverhältnismäßigem Aufwand verbunden ist (dies gilt insbesondere für die Verarbeitung für statistische Zwecke, vorbehaltlich geeigneter Bedingungen und Maßnahmen, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit), die Verarbeitung gesetzlich vorgesehen ist oder die personenbezogenen Daten dem Berufsgeheimnis unterliegen.

(3) Wahrgenommene Verletzungen des Schutzes personenbezogener und vertraulicher Daten sind unverzüglich zu melden. Die Meldung hat anlassfallspezifisch an die Vorgesetzten, die IT-Abteilung, die Leitung von Statistik Austria oder/und die/ den Datenschutzbeauftragte/n zu erfolgen

(4) Wenn durch die Verletzung des Schutzes personenbezogener Daten ein Risiko für die Rechte und Freiheiten von betroffenen Personen besteht, hat Statistik Austria unverzüglich und möglichst binnen 72 Stunden nachdem ihr die Verletzung bekannt wurde, eine Meldung mit den in Artikel 33 DSGVO genannten Inhalten (Beschreibung der Verletzung, Anzahl der betroffenen Personen bzw. der Datensätze, Maßnahmen, wahrscheinliche Folgen, Dokumentation etc.) an die Datenschutzbehörde zu erstatten. Wenn ein hohes Risiko für Rechte und Freiheiten von betroffenen Personen besteht, hat Statistik Austria zudem ohne ungebührliche Verzögerung die betroffenen Personen über die von ihr verursachten Datenschutzverletzungen zu benachrichtigen, falls nicht die Bedingungen gemäß Artikel 34 Abs. 3 (die Daten wurden unzugänglich gemacht werden, etwa durch Verschlüsselung; durch nachfolgende Maßnahmen ist sichergestellt, dass das hohe Risiko aller Wahrscheinlichkeit nach nicht mehr besteht; es wäre mit einem unverhältnismäßigen Aufwand verbunden wäre, in diesem Fall hat stattdessen eine

öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen) erfüllt sind.

(5) Wenn Statistik Austria als Auftragsverarbeiterin tätig ist, meldet sie eine bekanntgewordene Verletzung des Schutzes personenbezogener Daten unverzüglich dem Verantwortlichen.

5 RECHTE VON BETROFFENEN NATÜRLICHEN PERSONEN

(1) Bei Statistik Austria einlangende Begehren zur Wahrnehmung von Rechten betroffener Personen werden an die/ den Datenschutzbeauftragte/n weitergeleitet.

(2) Zur Durchführung der Betroffenenrechte (betrifft nicht die mit dem bereichsspezifischen Personenkennzeichen Amtliche Statistik (bPK-AS) pseudonymisierten personenbezogenen Daten) werden von jeder Leitung einer Organisationseinheit Kontaktpersonen genannt, über die die benötigten Informationen eingeholt werden.

(3) Betroffenen Personen stehen bezüglich ihrer nicht-pseudonymisierten personenbezogenen Daten folgende Betroffenenrechte zu, sofern diese Rechte aufgrund der rechtlichen Vorgaben im konkreten Fall zum Tragen kommen:

- Das Recht auf Auskunft (Art. 15 DSGVO): Die betroffene Person hat das Recht auf folgende Informationen: Ob personenbezogene Daten über sie verarbeitet werden; Verarbeitungszwecke; Datenkategorien; Kopie (z.B. Ausdruck) der verarbeiteten Dateninhalte; Datenempfänger oder Empfängerkategorien; geplante Speicherdauer (oder Kriterien für deren Festlegung); Bestehen eines Berichtigungs-, Löschungs-, Einschränkungs- oder Widerspruchsrechts; Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde; verfügbare Informationen über Datenherkunft; Bestehen einer automatisierten Entscheidungsfindung (Profiling eingeschlossen), Logik und Tragweite solcher Verfahren.

- Das Recht auf Berichtigung (Art. 16 DSGVO) betrifft die Dateninhalte.

- Das Recht auf Löschung (Art. 17 DSGVO) (einschließlich des „Rechts auf Vergessenwerden“): Das Löschungsrecht setzt voraus, dass einer der folgenden Umstände vorliegt oder eingetreten ist: Wegfall des Verarbeitungszwecks, Widerruf der Einwilligung der betroffenen Person und gleichzeitig fehlt es an einer anderweitigen Rechtsgrundlage der Verarbeitung, wirksamer Widerspruch gegen die Datenverarbeitung, anfängliche Unrechtmäßigkeit der Datenverarbeitung, rechtliche Verpflichtung zur Löschung (z.B. Gesetz, Urteil, Bescheid), Fehlen einer Einwilligung der Erziehungsberechtigten eines Kindes. Es besteht jedoch kein Recht auf Löschung („Vergessen")

für die betroffene Person, wenn die Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, erforderlich sind. Es gilt zudem nicht für Verarbeitungen zu statistischen Zwecken, wenn die Löschung die Erreichung der Verarbeitungsziele unmöglich oder schwerwiegend beeinträchtigen würde.

- Das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO): Es handelt sich um ein zeitlich beschränktes bzw. bedingtes Recht. Die Voraussetzungen sind: die Richtigkeit der Daten wird bestritten; die Rechtmäßigkeit der Datenverarbeitung wird bestritten, die betroffene Person selbst lehnt aber die Löschung ab; die betroffene Person benötigt die Daten, deren Verarbeitungszweck weggefallen ist, für die Geltendmachung von Rechtsansprüchen; die betroffene Person hat Widerspruch gegen die Datenverarbeitung eingelegt. Datenempfänger sind, wenn nicht unmöglich oder mit unverhältnismäßigem Aufwand verbunden, über Einschränkungen zu informieren. Die betroffene Person kann verlangen, über die Empfänger der Daten informiert zu werden.

- Das Recht auf Datenübertragbarkeit (Art. 20 DSGVO): Dieses Recht könnte nur dann zur Anwendung kommen, wenn Grundlage für die Datenverarbeitung entweder die Einwilligung der betroffenen Person oder ein Vertrag ist. Es gilt nicht für Verarbeitungen, die für die Wahrnehmung einer Aufgabe erforderlich sind, die im öffentlichen Interesse liegt.

- Das Recht auf Widerspruch (Art. 21 DSGVO): Dieses Recht gilt nicht für Verarbeitungen, zu denen die betroffene Person ihre Einwilligung gegeben hat, oder die für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, oder die zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, erforderlich sind. Kein Widerspruchsrecht für die betroffene Person besteht zudem, wenn die Verarbeitung zu statistischen Zwecken zur Ausführung einer Aufgabe aus Gründen des öffentlichen Interesses erforderlich ist.

6 AUFTRÄGE

(1) Zur Erteilung von Aufträgen sind nur die Leitung von Statistik Austria oder die gemäß Kapitel 2.1 festgelegten Personen berechtigt.

(2) Der Auftrag zur Verwendung personenbezogener Daten darf nur im Sinne der im Gesetz oder der Verordnung festgelegten Art erfolgen. Soweit kein rechtlicher Auftrag (z. B. Abonnentendateien, u.ä.) vorliegt, ist gemäß der erfolgten Dokumentation im Verzeichnis der Verarbeitungstätigkeiten der Auftrag zu erteilen. Die

Erteilung von Aufträgen (z.B. durch die Projekt- bzw. Bereichsleitung) an die IT-Abteilung hat in der in der Statistik Austria üblichen Form (z. B. Vordrucke, Dienstzettel, E-Mail, Jira) zu erfolgen.

(3) Für die erstmalige Inbetriebnahme von Rechnern ist ein eigener Auftrag an die IT-Abteilung erforderlich.

7 BELEHRUNGSPFLICHT

(1) Alle Bediensteten sind von der/ dem Datenschutzbeauftragte/n vor Aufnahme ihrer Tätigkeit über das Grundrecht auf Datenschutz, die gegenständliche Datensicherheitsvorschrift, die bestehenden Geheimhaltungspflichten (Datengeheimnis, Statistikgeheimnis, Amtsverschwiegenheit) sowie die Strafbestimmungen nachweislich zu belehren. Eine schriftliche Belehrung ist überdies anlässlich von Änderungen der aktuellen Fassung solcher Bestimmungen durchzuführen.

(2) Allen Benutzern von IT-Arbeitsgeräten ist von der/ dem Datenschutzbeauftragte/n das Verbot der Verwendung nicht freigegebener Software, gemäß Kapitel 10 Abs. (2), nachweislich zur Kenntnis zu bringen.

(3) Alle Personen, die regelmäßig Zutritt zu Betriebsräumen oder Rechnerräumen haben, sind, sofern sie nicht der üblichen Geheimhaltungspflicht unterliegen, von der/ dem Datenschutzbeauftragte/n über die bestehenden Geheimhaltungspflichten nachweislich zu unterrichten.

(4) Andere Personen, die nur fallweise Zutritt zu Betriebsräumen oder Rechnerräumen haben, sind von einer zutrittsberechtigten Begleitperson entsprechend der gültigen Datensicherheitsvorschrift auf die bestehenden Geheimhaltungsbestimmungen hinzuweisen.

(5) Einmal jährlich ist weiters eine Kurzbelehrung im Umlaufwege den Personen gemäß Kapitel 7 Abs. (1), (2) und (3) zu erteilen.

8 ZUTRITTSBESCHRÄNKUNG

(1) Die Zutrittsberechtigungen bzw. -beschränkungen richten sich nach der geltenden Sicherheitsordnung (z. B. Ausweispflicht) und den nachfolgenden Bestimmungen.

(2) Betriebsräume sind nach Möglichkeit außerhalb der Betriebszeiten zu versperren. Mangels einer Sperrmöglichkeit der Betriebsräume ist durch andere geeignete Maßnahmen (Abschalten des Gerätes, Aktivieren der Bildschirmsperre, Wegsperren der Datenträger, etc.) die Gefahr unberechtigter Zutritte zu verhindern.

(3) Betriebsräume dürfen nur von – durch den Leiter einer Organisationseinheit – autorisierten Personen auch alleine betreten werden. Alle anderen Personen müssen von autorisierten Bediensteten begleitet werden.

(4) Rechnerräume stellen besondere Sicherheitszonen dar. Sie müssen gegen unbefugten Zutritt gesichert sein. Schlüssel bzw. Ausweisberechtigungen dürfen nur an zutrittsberechtigte Personen vergeben werden. Für den Zutritt zu Rechnerräumen gilt Kapitel 8 Abs. (3) sinngemäß.

(5) Den Organen der Datenschutzbehörde ist der Zutritt zu den Betriebsräumen und Rechnerräumen in Begleitung dazu autorisierter Personen zu gestatten. Die Leitung von Statistik Austria und die/ der Datenschutzbeauftragte sind davon im Vorfeld zu verständigen.

9 ZUGRIFFSBESCHRÄNKUNG

(1) Der Zugriff auf eine IT-Anwendung darf nur unter Verwendung eines Berechtigungscodes ermöglicht werden. Der Berechtigungscode kann – je nach IT-Anwendung – ein Bedienerkennzeichen (BKZ) oder ein Passwort sein.

(2) Jede/r Benutzer/in hat ausschließlich ihre/ seine eigene Benutzerkennung und Passwort zu verwenden. Die Verwendung einer fremden Benutzerkennung oder Passwortes ist verboten. Lediglich für Vertretungszwecke ist dieses Passwort in einem verschlossenen Kuvert beim Leiter der Organisationseinheit zu deponieren. Nach Wegfall der Vertretungstätigkeit ist jedenfalls ein neues Passwort durch die/ den Benutzer/in festzulegen. In begründeten Fällen kann mit Zustimmung der Leitung von Statistik Austria ausnahmsweise ein gemeinsames Passwort (z. B. für Schreibpools) verwendet werden.

(3) Die Weitergabe des Passwortes an andere Personen ist verboten.

(4) Der Versuch, das Passwort einer/ eines Benutzerin/Benutzers herauszufinden, zieht dienstrechtliche Konsequenzen nach sich.

(5) Hat eine/ ein Bedienstete/r Anlass zur Vermutung, dass ihr/ sein Passwort oder das Passwort einer/ eines anderen Bediensteten anderen Personen bekannt ist, so hat sie/ er diesen Umstand der/ dem Datenschutzbeauftragten anzuzeigen; das Passwort ist in diesem Fall unverzüglich abzuändern.

(6) Das Passwort ist entsprechend der Passwortrichtlinie in periodischen Intervallen zu ändern. Passwörter dürfen nicht notiert werden und nur in von der IT-Abteilung freigegebenen Lösungen gespeichert werden (z.B. Passwortsafe). Einmal genutzte Passwörter dürfen nicht wieder verwendet werden, auch nicht bei

anderen Systemen. Gruppen- und Projektpasswörter sind zwingend und zeitnah zu ändern, wenn eine Person die Gruppe bzw. das Projekt verlässt.

(7) Leicht eruierbare Begriffe dürfen als Passwort nicht verwendet werden (z. B. Vornamen – weder eigene noch von Familienmitgliedern, Geburtsdaten etc.).

(8) Jede/r Anwender/in und jede/r Benutzer/in ist für ihr/ sein Passwort und somit auch für alle Eingaben verantwortlich, die unter ihrem/ seinem Passwort getätigt werden.

(9) Die Art und der Umfang der Zugriffsberechtigung (z. B. Lesen, Verändern, Kopieren, Löschen) sowie die Einräumung von Teilzugriffsmöglichkeiten auf Datenbestände ist für jede/ jeden Benutzer/in durch die Leitung der jeweiligen Organisationseinheit oder durch eine/n von dieser ermächtigten Bediensteten festzulegen.

(10) Die Leitung einer Organisationseinheit oder die Projektleiter hat gemäß dem Stand der technischen Möglichkeiten unter Verwendung der eingesetzten Standardsoftware und/oder durch organisatorische Schritte Maßnahmen zur Erstellung von Zugriffsprotokollen bei Verarbeitung besonders sensibler Daten zu setzen und die Nachvollziehbarkeit der einzelnen Verarbeitungsschritte zu gewährleisten.

10 BETRIEBSBESCHRÄNKUNG

(1) Beim Verlassen des Arbeitsplatzes ist durch geeignete Maßnahmen (z. B. Abschalten des Gerätes, Aktivieren der Bildschirmsperre, Versperren des Raumes) sicherzustellen, dass das Datenendgerät nicht durch Unbefugte in Betrieb genommen werden kann.

(2) Auf IT-Arbeitsmitteln ist nur die für den jeweiligen Arbeitsplatz vorgesehene und freigegebene Originalsoftware zu verwenden. Das Einspielen privater Software ist untersagt, um insbesondere die Gefahr der Einschleppung von Schadsoftware zu minimieren und um daraus möglicherweise resultierende Schäden zu vermeiden.

(3) Datenträger mit personenbezogenen Daten sind außerhalb der Verwendung versperrt zu halten.

(4) Unbrauchbare Datenträger sind an die ausgebende Stelle zu retournieren und von dieser so zu entsorgen, dass eine missbräuchliche Verwendung auszuschließen ist.

11 PROTOKOLLIERUNG

(1) Bei IT-Anwendungen ist die Protokollierung aller mit der Anwendung durchgeführten Verwendungsvorgänge (z. B. Änderungen, Abfragen etc.) automationsunterstützt vorzusehen, jedoch unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit. Darüber hinausgehende Verwendungen, insbesondere Übermittlungen, sind gesondert zu protokollieren.

(2) Protokoll- und Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck – das ist die Kontrolle der Zulässigkeit der Verwendung des protokollierten oder dokumentierten Datenbestandes – unvereinbar sind. Unvereinbar ist insbesondere die Weiterverwendung zum Zweck der Kontrolle von Betroffenen, deren Daten im protokollierten Datenbestand enthalten sind, oder zum Zweck der Kontrolle jener Personen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung, es sei denn, dass es sich um die strafrechtliche Verfolgung eines Verbrechens gemäß StGB handelt.

(3) Sofern gesetzlich nicht ausdrücklich anderes angeordnet ist, sind Protokoll- und Dokumentationsdaten drei Jahre lang aufzubewahren. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung oder Dokumentation betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird.

12 DATENSICHERUNG UND DATENAUSLAGERUNG

(1) Die folgenden Maßnahmen zur Datensicherung und Datenauslagerung sind von der Projektleitung zu ergreifen bzw. zu veranlassen, soweit die technischen Möglichkeiten gegeben sind und diese verfahrensmäßig vorgesehen sind:

a) Zum Zwecke der Wiederherstellung von Daten und Programmen und zur Ermöglichung von Korrekturen sind über selbsterstellte Prozeduren aus Standardfunktionen der eingesetzten Softwarewerkzeuge und über selbstentwickelte Programme sowie über gespeicherte Datenbestände in jeweils angemessenen Zeitabständen Sicherungskopien anzulegen.

b) Sicherungskopien sind getrennt von den Originalen, geschützt gegen Diebstahl, aufzubewahren.

c) Desgleichen sind Belege, deren Verarbeitung durch Kopien abgesichert sind, nach den Bestimmungen des Abs. (1) b) aufzubewahren.

d) Für Daten mit hohen Wiederbeschaffungskosten sind erforderlichenfalls mehrere Sicherungskopien anzulegen und außerhalb von Statistik Austria

(disloziert, z. B. im Zentralen Ausweichsystem des Bundes (ZAS)) aufzubewahren.

(2) Die Projektleitungen haben gemäß Abs. (1) a) – d) jene Maßnahmen unter Bedachtnahme, wie hoch die Wahrscheinlichkeit eines Risikofalles und das Ausmaß der Folgen zu bewerten ist, zu ergreifen.

(3) Alle dienstlich relevanten Daten sind auf die von der IT-Abteilung zur Verfügung gestellten Netzlaufwerke zu speichern. Die Sicherung vor Fremdzugriffen und das Verhindern von Verlust der auf einem IT-Endgerät gespeicherten Daten haben in Eigenverantwortung zu erfolgen. Schützenswerte Daten auf unverschlüsselten elektronischen Datenträgern außer Haus zu bringen ist verboten.

13 KONTROLLE

(1) Für die Kontrolle der Einhaltung der Bestimmungen gegenständlicher Datensicherheitsvorschrift sind die jeweiligen Vorgesetzten der Mitarbeiterinnen und Mitarbeiter sowie die/ der Datenschutzbeauftragte zuständig.

(2) Über die getroffenen Maßnahmen sind von der Projektleitung bzw. den von ihr bestimmten Mitarbeitern und Mitarbeiterinnen Aufzeichnungen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

(3) Über die Art und den Umfang der durchgeführten Kontrollen sind von der Projektleitung bzw. den von ihr bestimmten Mitarbeitern und Mitarbeiterinnen Aufzeichnungen zu führen und den/die betroffene(n) Bedienstete(n) davon in Kenntnis zu setzen sowie ein Protokoll auszuhändigen.

(4) Über anlässlich von Kontrollen festgestellte schwerwiegende Unzulänglichkeiten ist die Leitung von Statistik Austria und/oder die/ der Datenschutzbeauftragte umgehend zu informieren.

14 INKRAFTTRETEN

Die neue Fassung der Datensicherheitsvorschrift ersetzt jene vom 1. März 2003 und tritt mit dem 25. Mai 2018 in Kraft.

Dr. Konrad Pesendorfer (e.h.) Dr. Gabriela Petrovic (e.h.)

(Leitung von Statistik Austria)