



Bundesgesetz über den Datenschutz, Änderung vom 24. März 2006: Häufig gestellte Fragen zur Umsetzung bei der Datenbearbeitung durch Private

1. Allgemeines

11 Müssen bestehende Bearbeitungen bzw. Datensammlungen an die Änderungen angepasst werden?

Die mit der Änderung vorgesehenen Neuerungen unterscheiden nicht zwischen bestehenden und neuen Datensammlungen bzw. Bearbeitungen. Soweit bestehende Datensammlungen weiterhin operativ genutzt werden und bestehende Bearbeitungen weiter durchgeführt werden, sind Anpassungen an die geänderte Rechtslage vorzunehmen. Dazu folgende Hinweise:

- Erkennbarkeit, Informationspflicht: Für die gegebenenfalls notwendigen Massnahmen zur Gewährleistung der Erkennbarkeit bzw. Information der betroffenen Personen (vgl. unten, Ziff. 2) besteht eine Übergangsfrist von einem Jahr.
- Bekanntgabe ins Ausland: Wo Personendaten in Staaten bekannt gegeben werden, die keine Gesetzgebung kennen, welche einen angemessenen Schutz gewährleistet, ist zu prüfen, ob Garantien des Empfängers (etwa durch entsprechende vertragliche Bestimmungen) einzuholen sind (vgl. unten, Ziff. 4). Vom Einholen von Garantien kann abgesehen werden, wenn eine der übrigen Ausnahmebestimmungen des neuen Art. 6 Abs. 2 DSG erfüllt ist (insb. Vorliegen einer Einwilligung der Betroffenen oder Bekanntgabe innerhalb eines Konzerns, der angemessene Datenschutzregeln kennt).
- Meldepflicht der Datensammlungen: Künftig sind in gewissen Fällen Datensammlungen meldepflichtig, die bisher ausgenommen waren (vgl. unten, Ziff. 7). Für diese Fälle wird der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) die Übergangsregelung von Art. 38 des geltenden DSG analog anwenden; d.h. es besteht eine Frist von einem Jahr für die Meldung.

Verweise: Art. 4 Abs. 4, 7a revDSG, BBI 2003 2147 (Erkennbarkeit, Informationspflicht); Art. 6 revDSG, Art. 5 revVDSG, BBI 2003 2128 ff. (Übermittlung ins Ausland); Art. 11a revDSG, Art. 1–4 revVDSG, BBI 2137 f.

12 Wie weit kann sich ein Anwender in einem Zweifelsfall bei der Auslegung des revidierten DSG an der Auslegung der EU-Datenschutzrichtlinie 95/46/EG durch eine ausländische Datenschutzbehörde ausrichten?

Die Revision bringt in verschiedenen Punkten eine Annäherung des schweizerischen Rechts an die EU-Datenschutzrichtlinie. Die Auslegung der Datenschutzrichtlinie durch ausländische Datenschutzbehörden oder die durch Gruppe nach Art. 29 der Richtlinie kann in diesen Fällen Hinweise auf die praktische Anwendung geben. Soweit es um die Konkretisierung der materiellen Datenschutzgrundsätze geht, kann in der Regel davon ausgegangen werden,

dass bei einem mit der Richtlinie konformen Vorgehen des Datenbearbeiters auch die Anforderungen des DSGVO erfüllt werden.

2. Transparenz

21 Erkennbarkeit der Beschaffung und Bearbeitung (Art. 4 Abs. 4)

211 Unter welchen Voraussetzungen ist die Erkennbarkeit gegeben?

Mit dem neuen Art. 4 Abs. 4 tritt gegenüber dem geltenden Recht keine grundsätzliche Neuerung ein. Bereits bisher wurde aus dem Grundsatz von Treu und Glauben (Art. 4 Abs. 2 DSGVO) abgeleitet, dass die Beschaffung, der Zweck der Bearbeitung und die Identität des Datenbearbeiters erkennbar sein müsse. In vielen Fällen, insb. bei alltäglichen Transaktionen, werden keine besonderen Massnahmen erforderlich sein. Massgeblich ist, ob ein (fiktiver) durchschnittlicher Adressat oder Kunde aufgrund der konkreten Gegebenheiten im Einzelfall erkennen kann, dass, von wem und zu welchem Zweck Daten beschafft werden und an wen sie gegebenenfalls weitergeleitet werden.

Verweise: Art. 4 Abs. 4, BBl 2003 2124 ff.

212 Zu welchem Zeitpunkt muss die Erkennbarkeit gewährleistet werden?

Grundsätzlich muss die Beschaffung in dem Zeitpunkt erkennbar sein, in dem sie erfolgt; zumindest muss der genaue Zeitpunkt absehbar sein, an dem bestimmte Daten beschafft werden.

Wenn jedoch das Erkennbarmachen im Beschaffungszeitpunkt den Zweck der Bearbeitung vereiteln würde oder es aus anderen Gründen dem Datenbearbeiter nicht zuzumuten ist, den genauen Zeitpunkt der Beschaffung anzugeben (namentlich, weil dies einen sehr grossen Aufwand verursachen würde), sind – je nach den Umständen im konkreten Fall – zwei Vorgehensweisen möglich. Entweder wird eine später erfolgende Beschaffung durch entsprechende allgemeine Hinweise oder vertragliche Bestimmungen vorgängig erkennbar gemacht. Oder aber sie wird nachträglich erkennbar gemacht.

Je heikler die betreffenden Personendaten sind, desto eher ist dem Datenbearbeiter ein Erkennbarmachen im Zeitpunkt der Beschaffung zuzumuten bzw. desto gewichtiger muss sein Interesse sein, das Erkennbarmachen nicht im Zeitpunkt der Beschaffung vorzunehmen.

Ist im Rahmen einer Transaktion (z.B. bei einem Vertragsschluss) noch nicht klar, ob später eine Beschaffung von zusätzlichen Daten erfolgen muss (bzw. besteht lediglich die Möglichkeit, dass später zusätzliche Daten beschafft werden), so gelten die gleichen Grundsätze; d.h., in der Regel sind die Betroffenen im konkreten Zeitpunkt der Beschaffung zu informieren. Ein blosser Hinweis auf die Möglichkeit einer später erfolgenden Datenbeschaffung reicht namentlich dann grundsätzlich nicht aus, wenn besonders schützenswerte Personendaten oder Persönlichkeitsprofile beschafft und bearbeitet werden.

Die hier skizzierten Grundsätze gelten auch für die Information nach Art. 7a (vgl. Ziff. 222).

213 Kann die Weitergabe von Daten innerhalb des gleichen Konzerns generell als erkennbar gelten?

Nein, es kann nicht ohne Weiteres davon ausgegangen werden, dass eine solche Weitergabe – auch wenn es sich um eine Weitergabe innerhalb derselben Rechtsperson handelt – für

die betroffenen Personen erkennbar ist. Wenn z.B. zwei Unternehmensteile in unterschiedlichen Geschäftsbereichen tätig sind oder mit unterschiedlichen Bezeichnungen gegen aussen auftreten, muss die Erkennbarkeit mit geeigneten Massnahmen sichergestellt werden.

214 Unter welchen Voraussetzungen können Daten beschafft und bearbeitet werden, ohne dass dies erkennbar gemacht wird?

Wenn ein besonderes, überwiegendes Interesse des Datenbearbeiters daran besteht, Personendaten ohne Wissen der Betroffenen zu beschaffen und zu bearbeiten, kann vom Erkennbarmachen abgesehen werden. Ein solches überwiegendes Interesse des Datenbearbeiters kann aber nur geltend gemacht werden, wo das blosser Erkennbarmachen den Zweck der Bearbeitung vereiteln würde. Wo dies praktikabel ist, muss in einer generellen Art und Weise) vorab darauf aufmerksam gemacht werden, dass unter bestimmten Umständen eine heimliche Beschaffung vorgenommen werden kann; die Umstände müssen so genau wie möglich umschrieben werden. Die Information kann beispielsweise beim Abschluss eines Vertrags vorgenommen werden (wenn ein Vertragsverhältnis mit den Betroffenen besteht) oder sie kann im Rahmen einer Weisung an die Mitarbeiterinnen und Mitarbeiter erfolgen (wenn es etwa um die Bekämpfung von Missbräuchen der Kommunikationsinfrastruktur des Arbeitgebers geht)..

Auch eine gesetzliche Bestimmung kann vorsehen, dass Daten beschafft werden dürfen, ohne dass dies für die Betroffenen erkennbar ist.

215 Wie ist – z.B. im Falle einer Firmenübernahme – bei der Integration fremder Datenbestände in eigene Datensammlungen vorzugehen?

Ändert der Inhaber der Datensammlung, so ändert sich eine wesentliche Rahmenbedingung der Bearbeitung. Der Wechsel muss für die Personen, deren Daten bearbeitet werden, erkennbar sein. Je nach Art der bearbeiteten Daten und Zweck der Bearbeitung können – auch wenn der Bearbeitungszweck gleich bleibt und die Daten bisher rechtmässig bearbeitet wurden – unterschiedliche Massnahmen erforderlich sein. Eine Abstufung lässt sich wie folgt skizzieren:

- Für die blosser Bearbeitung von Daten, die ohnehin öffentlich zugänglich oder aus anderen Gründen wenig sensibel sind (z.B. die Bearbeitung von Adressdaten zu Werbezwecken) ist die Erkennbarkeit bereits gegeben, wenn ohnehin eine Kommunikation mit den Betroffenen stattfindet (z.B. personalisierter Versand von Werbematerial).
- Handelt es sich um heiklere Daten, die wesentliche Interessenbereiche der betroffenen Person tangieren können (etwa Kundendaten einer Bank oder Versicherung), so ist es angezeigt, die Mitteilung über den Wechsel des Inhabers der Datensammlung vorgängig durchzuführen und den Betroffenen die Möglichkeit zu geben, die Datenweitergabe abzulehnen.
- Handelt es sich um besonders schützenswerte Personendaten, so ist gemäss Art. 7a zu informieren (vgl. Ziff. 3 unten) und ausdrücklich darauf hinzuweisen, dass die Datenweitergabe abgelehnt werden kann.

Verweise: Art. 4 Abs. 4, 7a revDSG; BBl 2124 ff., 2131 ff.; 5. Tätigkeitsbericht EDÖB, 53.

216 Wie ist bei der Beschaffung bei Dritten vorzugehen?

Auch die Beschaffung bei einer Drittperson muss für die Betroffenen grundsätzlich erkennbar sein. Die Erkennbarkeit kann in solchen Fällen auch vorab, etwa durch entsprechende Informationen in einem Vertrag oder in Allgemeinen Geschäftsbedingungen (AGB) gewährleistet werden.

217 Ist die Erkennbarkeit auch zu gewährleisten, wenn Daten aus allgemein zugänglichen Quellen (z.B. im Internet) beschafft werden?

Werden Daten aus allgemein zugänglichen Quellen beschafft, so sind grundsätzlich keine weiteren Massnahmen zur Gewährleistung der Erkennbarkeit der Beschaffung und Bearbeitung nötig. Dagegen kann sich eine Informationspflicht ergeben, wenn solche Daten zu Persönlichkeitsprofilen zusammengestellt werden (vgl. unten, Ziff. 22). Zu berücksichtigen ist zudem, dass Daten nicht für Zwecke beschafft werden dürfen, bezüglich derer die Betroffenen die Bearbeitung ausdrücklich untersagt haben.

22 Informationspflicht beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen (Art. 7a)

221 Welche Informationen müssen den betroffenen Personen angegeben werden?

Abs. 2 des neuen Art. 7a umschreibt den Minimalumfang der Information: Inhaber der Datensammlung, Zweck des Bearbeitens und die Kategorien allfälliger Datenempfänger. Je nach Kontext sind die Betroffenen etwa auch darüber zu informieren, ob die Angabe der Daten obligatorisch ist und welche Folgen die Verweigerung der Angabe der Daten hat.

Nicht angegeben werden müssen Angaben zur Identität der einzelnen Datenempfänger.

Verweise: Art. 7a Abs. 2 revDSG; BBI 2003 2131 ff.

222 Wann und wie muss die Information erfolgen?

Die Information muss grundsätzlich gleichzeitig mit der Beschaffung erfolgen. Für weitere Hinweise betreffend den Zeitpunkt der Information vgl. oben, Ziff. 212.

Die Information muss ausdrücklich erfolgen. Eine bestimmte Form ist zwar nicht vorgeschrieben. Zwar wird in der Regel die schriftliche Form sinnvoll sein, eine mündliche Information ist aber grundsätzlich ebenfalls möglich (z.B. bei einer telefonischen Umfrage oder bei der telefonischen Konsultation eines medizinischen Beratungszentrums).

Verweise: Art. 7a revDSG; BBI 2003 2131 ff.

223 Unter welchen Voraussetzungen können Daten beschafft und bearbeitet werden, ohne dass die Betroffenen darüber informiert werden müssen?

Die Information der Betroffenen bei der Beschaffung kann dann unterbleiben – bzw. zu einem späteren Zeitpunkt erfolgen – wenn ein Gesetz dies vorsieht, wenn es wegen überwiegender Interessen Dritter erforderlich ist oder wenn eigene überwiegende Interessen des Datenbearbeiters es erfordern und er die betreffenden Personendaten nicht Dritten bekannt gibt (vgl. dazu auch oben, Ziff. 212, 214 und 222).

Verweise: Art. 7a, 9 revDSG; BBI 2003 2131 ff.

224 Wann muss informiert werden, wenn Daten beschafft werden, die sich erst mit der Zeit zu einem Persönlichkeitsprofil verdichten?

Die Information hat so früh wie möglich zu erfolgen. Sobald vom Zweck der Bearbeitung her ersichtlich ist, dass möglicherweise Persönlichkeitsprofile entstehen können, sind die betroffenen Personen entsprechend zu informieren.

225 Muss nach der neuen Bestimmung informiert werden, wenn eine Bearbeitung bereits vor dem Inkrafttreten der Revision durchgeführt wurde (bzw. wenn die zugrunde liegende Datensammlung bereits im Zeitpunkt des Inkrafttretens bestand)?

Nein, die Informationspflicht gilt nicht rückwirkend für bereits beschaffte Daten. Hingegen muss gemäss dem neuen Art. 7a informiert werden, wenn im Zusammenhang mit bereits bisher vorgenommenen Bearbeitungen zusätzliche Daten beschafft werden (sofern die Betroffenen nicht bereits früher hinreichend informiert wurden) oder wenn Daten von Personen beschafft werden, die bisher nicht von einer bereits vor Inkrafttreten der Revision durchgeführten Bearbeitung betroffen waren.

Verweis: BBI 2003 2147.

3. Definition der Einwilligung (Art. 4 Abs. 5)

31 Ist für die Bearbeitung von Personendaten in jedem Fall eine Einwilligung der betroffenen Person erforderlich?

Nein. Bei Art. 4 Abs. 5 handelt es sich lediglich um eine Begriffsdefinition. Sie umschreibt die Kriterien, denen eine rechtsgültige Einwilligung genügen muss, wenn das Gesetz die Bearbeitung von der Einwilligung der Betroffenen abhängig macht (Art. 6 Abs. 2 Bst. b [neu], 13 Abs. 1, 17 Abs. 2 Bst. c, 19 Abs. 1 Bst. b DSGVO).

32 Wann ist die Information, gestützt auf die die Einwilligung erfolgt, angemessen?

Die Personen, deren Daten bearbeitet werden, müssen einerseits über die Rahmenbedingungen der Bearbeitung informiert werden (vgl. oben, Ziff. 211 und 221), andererseits müssen sie über die Folgen der Nichtzustimmung in Kenntnis gesetzt werden (soweit diese nicht ohne Weiteres absehbar sind), insb. über Nachteile, die sie in diesem Fall erleiden können. Die betroffenen Personen müssen über alle Informationen verfügen, die erforderlich sind, damit sie ihren Willen in Kenntnis der entscheidungsrelevanten Punkte zum Ausdruck bringen können.

Die Information kann auf verschiedensten Wegen vermittelt werden: Schriftlich (auf Papier, am Bildschirm, per SMS), telefonisch oder auch mündlich. Es besteht kein Formerfordernis.

33 Wann ist eine Einwilligung freiwillig?

Die Einwilligung kann grundsätzlich dann als freiwillig gelten, wenn die mit der Nichtzustimmung verbundenen Nachteile keinen sachlichen Zusammenhang zum Zweck der Bearbeitung stehen oder diesem gegenüber unverhältnismässig sind.

Verweis: BBI 2003 2127.

34 In welcher Form muss die Einwilligung erfolgen?

Die Einwilligung ist nicht an eine bestimmte Form gebunden; insb. kann sie grundsätzlich auch stillschweigend bzw. durch konkludentes Handeln erfolgen. Geht es um die Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen, so muss die Einwilligung ausdrücklich erfolgen. Aus Beweisgründen ist in diesen Fällen die schriftliche Form zu empfehlen. Eine Einwilligung auf elektronischem Weg, also z.B. mittels Mausklick auf einem Webformular, ist sowohl bei einfachen Daten als auch bei besonders schützenswerten Daten oder Persönlichkeitsprofilen grundsätzlich zulässig (sofern Rahmenbedingungen und Abläufe so gestaltet werden, dass die Authentifizierung der betroffenen Person

und die Sicherheit der Übermittlung angemessen sichergestellt werden).

Verweis: BBI 2003 2127 f.

4. Grenzüberschreitende Bekanntgabe (Art. 6)

41 Welche Konsequenzen hat die Änderung der verwendeten Begriffe?

Der Wortlaut von Art. 6 DSG wird insofern geändert, als bisher an der Übermittlung von Datensammlungen angeknüpft wurde. Dem gegenüber wird neu auf die Bekanntgabe von „Personendaten“ ganz generell Bezug genommen. In der Praxis bedeutet dies keine wesentliche Änderung, denn jeder Informationsbestand, der Daten betreffend mehr als nur eine einzige Person umfasst, ist bereits nach bisherigem Verständnis grundsätzlich eine Datensammlung.

Bisher lautete die Bestimmung so, dass von einer schwerwiegenden Gefährdung der Betroffenen namentlich dann auszugehen ist, wenn im Empfangsland ein „Datenschutz“ fehlt, der dem schweizerischen gleichwertig ist. Neu wird am Fehlen einer „Gesetzgebung“ angeknüpft, die einen angemessenen Schutz gewährleistet. Dies ist das ausschlaggebende Kriterium; ist es nicht gegeben, so kann die Bekanntgabe ins Ausland nur stattfinden, wenn eine der im neuen Art. 6 Abs. 2 DSG aufgezählten Bedingungen erfüllt ist. Damit wird namentlich die Verpflichtung der Datenbearbeiter verstärkt, in solchen Fällen dafür zu sorgen, dass der Schutz von Personendaten hinreichend gewährleistet ist.

Verweise: Art. 6 revDSG; BBI 2003 2128 ff..

42 Ist ein Abweichen von Art. 6 weiterhin möglich, wenn der Datenbearbeiter überwiegende Interessen geltend machen kann?

Bisher konnte der Datenbearbeiter vom grundsätzlichen Verbot der Übermittlung in ein Empfangsland, das keinen gleichwertigen Datenschutz kennt, gestützt auf einen Rechtfertigungsgrund – nach dem nicht abschliessenden Katalog in Art. 13 DSG namentlich jedes überwiegende private Interesse – abweichen. Der neue Art. 6 Abs. 2 hingegen zählt die Bedingungen einer rechtmässigen Übermittlung in einen Empfangsstaat, der keine Gesetzgebung kennt, die einen angemessenen Schutz gewährleistet, abschliessend auf. Der Datenbearbeiter muss bei Fehlen einer Datenschutzgesetzgebung im Empfangsland, die einen hinreichenden Schutz bietet, in jedem Fall zumindest für hinreichende Garantien sorgen, um den Datenschutz zu gewährleisten (sofern nicht eine der übrigen Bedingungen erfüllt ist).

43 Ist die Publikation von personenbezogenen Informationen auf Internet eine Bekanntgabe ins Ausland?

Wenn Personendaten auf Internet oder über andere automatisierte Informations- und Kommunikationsdienste der Öffentlichkeit allgemein zugänglich gemacht werden, so gilt dies nicht als Übermittlung ins Ausland. Bei der Veröffentlichung von Personendaten auf Internet zum Zweck der Information der Öffentlichkeit, namentlich durch die Medien, ist die Tatsache, dass diese Informationen auch im Ausland abgerufen werden können bloss ein Nebeneffekt. Selbstverständlich sind dabei die übrigen rechtlichen Anforderungen, die sich namentlich aus dem übrigen Datenschutz- und Persönlichkeitsrecht ergeben, zu beachten.

Verweis: Art. 5 revVDSG.

44 Was bedeutet das Erfordernis der Einwilligung bzw. Bekanntgabe „im Einzelfall“

Die Formulierung „im Einzelfall“ ist so zu interpretieren, dass auch eine Gesamtheit bzw. eine Mehrzahl von Bekanntgaben welche Personendaten derselben Person unter gleichen Voraussetzungen (Empfänger, Zweck, allfällige Weiterleitung) betrifft, erfasst werden kann,

etwa im Rahmen einer Einwilligung. Die Formulierung weist weiter darauf hin, dass die einzelne Bekanntgabe sich jeweils auf einen konkreten Fall – z.B. der Feststellung eines Rechtsanspruches vor Gericht – beziehen muss.

Verweis: BBl 2003 2128 ff.

45 Wann steht eine Bekanntgabe im „unmittelbaren Zusammenhang“ mit dem Abschluss oder der Abwicklung eines Vertrags?

In unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages stehen zunächst Datenbearbeitungen, die sich auf den von den beteiligten Parteien beabsichtigten Abschluss eines Vertrags beziehen (etwa eine Offertstellung). Die Abwicklung eines Vertrags umfasst die Erfüllung der vertraglichen Haupt- und Nebenpflichten. Die Bekanntgabe ist zulässig, wenn die aus dem Vertrag sich ergebenden Leistungen eine solche Bekanntgabe umfassen oder voraussetzen. Dabei ist z.B. zu denken an die Bekanntgabe von Personendaten des Vertragspartners an Kreditauskunfteien zur Bonitätsprüfung, an eine Datenübermittlung durch Spediteure im Zusammenhang mit der Lieferung von Gütern, Aufträge im internationalen Zahlungsverkehr, internationale Beförderungsleistungen (Bahn-, Schiffs- oder Flugreisen); Buchungen von Hotels, Mietwagen.

46 Wann muss der Datenbearbeiter davon ausgehen, dass die betroffene Person die Bearbeitung öffentlich zugänglich gemachter Daten untersagt hat?

Wünscht jemand, dass eine weitere Bearbeitung seiner durch ihn oder sie selbst veröffentlichten Daten zu bestimmten Zwecken nicht erfolgt oder will jemand seine Daten nur im Hinblick auf die Bearbeitung zu bestimmten Zwecken vornehmen, so muss er oder sie bei diesen Daten eine Mitteilung anbringen, welche die Einschränkung für die weitere Verwendung zum Ausdruck bringt. Zudem ist denkbar, dass die betroffene Person einem spezifischen Datenbearbeiter die Mitteilung macht, dass sie eine Bearbeitung ihrer veröffentlichten Daten nicht wünscht (vgl. auch Art. 12 Abs. 2 Bst. b DSGVO).

47 Welche Anforderungen müssen konzernweite Datenschutzregeln erfüllen, damit sie das Fehlen einer angemessenen Datenschutzgesetzgebung kompensieren können?

Damit konzernweite Datenschutzregeln das Fehlen einer angemessenen Datenschutzgesetzgebung im Empfangsland kompensieren können, müssen sie folgende Anforderungen erfüllen:

- materiell müssen sie mindestens die für private Datenbearbeiter relevanten Anforderungen des Europäischen Datenschutzübereinkommens STE 108 und des Zusatzprotokolls erfüllen;
- die Verbindlichkeit der Regeln für die einzelnen Konzerngesellschaften muss formell und bei der Anwendung in der Praxis sichergestellt sein;
- der EDÖB muss über die Regeln informiert sein.

Die formelle Verbindlichkeit kann beispielsweise durch einen Beschluss des Verwaltungsrates erreicht werden. Die einzelnen Gesellschaften müssen die Regeln übernehmen und implementieren. Die Sicherstellung der Anwendung in der Praxis kann beispielsweise durch interne Audits sichergestellt werden.

In einigen (europäischen) Staaten wird vorgesehen, dass konzernweite Datenschutzregeln von der jeweils zuständigen Datenschutzaufsichtsbehörde genehmigt werden müssen. Das schweizerische Recht sieht dagegen keine Genehmigung durch den EDÖB vor. Er muss lediglich informiert werden. Das schweizerische Recht verlangt auch nicht, dass die Regeln von der zuständigen Datenschutzaufsichtsbehörde im Empfangsland (oder den Empfangs-

ländern) genehmigt wurden.

48 Wie muss der EDÖB über Garantien und konzernweite Datenschutzregeln informiert werden?

Die Information des EDÖB muss nicht für jede einzelne Datenbekanntgabe erfolgen. Sie kann generell vorgenommen werden, wenn Bekanntgaben in einem bestimmten Bereich regelmässig gestützt auf bestimmte Standardverträge oder -Klauseln erfolgen.

Solange einmal gemeldete Datenschutzregeln einen angemessenen Schutz gewährleisten, müssen vorgenommene Anpassungen nicht jedes Mal gemeldet werden.

Werden von einem Datenbearbeiter generell die vom EDÖB anerkannte Standardverträge oder -Klauseln verwendet, so reicht eine einmalige diesbezügliche Information aus. Der EDÖB wird eine Liste der anerkannten Verträge und Klauseln veröffentlichen. Anerkannt werden auf jeden Fall die Modelle der EU, des Europarates sowie die vom EDÖB selbst mit erarbeiteten Klauseln (vgl. dazu auch den Website des EDÖB: <http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=de>).

Die Information kann auf elektronischem Weg erfolgen. Der EDÖB wird über die Modalitäten rechtzeitig informieren.

Der EDÖB prüft die Garantien und Datenschutzregeln, die ihm mitgeteilt werden und teilt dem Inhaber der Datensammlung das Ergebnis der Prüfung innert 30 Tagen ab Empfang der Information mit. Wenn nach dieser Frist keine Rückfrage erfolgt oder keine Vorbehalte geäussert wurden, können die Datenbearbeiter davon ausgehen, dass die Garantien oder konzernweiten Datenschutzregeln die Anforderungen erfüllen.

Verweise: Art. 6 revDSG; Art. 6 revVDSG; BBI 2003 2128 ff.

49 Ist die vom EDÖB zu führende Liste der Staaten, deren Gesetzgebung einen angemessenen Datenschutz gewährleistet, verbindlich und abschliessend?

Ein Datenbearbeiter, der Daten in einen auf der Liste aufgeführten Staat übermitteln, kann sich darauf berufen, gutgläubig zu handeln. Weiss er aber, z.B. aufgrund seiner Erfahrungen in der Praxis, dass in einem solchen Staat Datenschutzvorschriften – generell oder in bestimmten Bereichen – nicht beachtet werden, so ist er nicht mehr gutgläubig.

Die Liste hat keinen abschliessenden Charakter, zumal auch denkbar ist, dass in gewissen Staaten lediglich in spezifischen Sachgebieten eine angemessene Gesetzgebung besteht.

Verweis: Art. 7 revVDSG.

5. Auskunftsrecht (Art. 8 Abs. 2)

51 Besteht künftig eine Verpflichtung, die Herkunft der Daten in der Datensammlung festzuhalten?

Nein, eine solche Verpflichtung besteht nicht. Gemäss dem Wortlaut des geänderten Art. 8 Abs. 2 Bst. a DSG beschränkt sich das Auskunftsrecht, auf die „verfügbaren“ Angaben über die Herkunft der Daten. Es steht dem Datenbearbeiter frei, solche Angaben zu erfassen. Indessen würde es gegen Treu und Glauben verstossen, wenn diese Angaben bei Eintreffen eines Auskunftsgesuchs gelöscht würden, nur um darüber nicht Auskunft erteilen zu müssen.

Verweise: Art. 8 Abs. 2 revDSG; BBI 2003 2134 f.

52 Ist der „Quellenschutz“ künftig nicht mehr möglich?

Würde die Auskunft über die Datenherkunft gegen überwiegende Interessen Dritter verstossen, so kann die Auskunft nach Art. 9 DSGVO diesbezüglich eingeschränkt werden. Dasselbe gilt, wenn die Auskunfterteilung gegen überwiegende eigene Interessen des Datenbearbeiters verstossen würde; Voraussetzung ist, dass die Daten nicht an Dritte weitergeleitet werden.

Überwiegende Interessen Dritter können beispielsweise vorliegen, wenn Anhaltspunkte bestehen, dass die betroffene Person gegenüber einem Informanten gewalttätig werden könnte oder wenn die betroffene Person die Chefin oder der Chef des Informanten ist, dieser sich also in einem Abhängigkeitsverhältnis befindet. Besteht lediglich die Gefahr, dass für die Dritten Unannehmlichkeiten entstehen könnten, ist indessen ein überwiegendes Interesse zu verneinen.

53 Können künftig die Betroffenen generell die Erteilung der Auskunft auf elektronischem Weg verlangen?

Das Auskunftsbegehren muss nur dann elektronisch entgegengenommen werden, wenn der Datenbearbeiter dies ausdrücklich vorsieht, etwa indem er im Rahmen seines Internetauftritts oder in seinen Allgemeinen Geschäftsbedingungen darauf hinweist, dass Auskunftsbegehren über Mail an eine bestimmte Stelle oder mit einem Webformular gestellt werden können und entsprechende Identifizierungs- und Sicherheitsmechanismen eingerichtet werden.

Verweise: Art. 1 Abs. 2 revVDSG.

6. Datenbearbeitung durch Dritte (Art. 10a)

Welche Pflichten hat der Auftraggeber gegenüber dem Auftragnehmer?

Bezüglich den Anforderungen an eine Datenbearbeitung durch Dritte (Outsourcing) ergeben sich keine grundsätzlichen Änderungen gegenüber dem geltenden Recht. Die neue Bestimmung sieht indessen vor, dass die Auftragsdatenbearbeitung durch Gesetz oder Vereinbarung vorgesehen sein muss. Für die Privaten bedeutet das, dass die Auftragserteilung vertraglich erfolgen muss.

Verdeutlich wird im Gesetz auch die Verpflichtung des Auftraggebers, sich zu vergewissern, dass der Auftragnehmer dieselben Datenschutz- und Datensicherheitsstandards anwendet, wie er es selbst tun müsste. Zudem muss er sich vergewissern, dass die notwendigen Massnahmen in der Praxis auch getroffen werden, etwa, indem er dies vor Ort überprüft. Hingegen ist der Auftraggeber nicht dazu verpflichtet, die Datenbearbeitung durch den Auftragnehmer permanent zu überwachen. Verfügt der Auftragnehmer über eine Zertifizierung nach der Verordnung vom 28. September 2007 über die Datenschutzzertifizierungen, so kann der Auftraggeber davon ausgehen, dass die Bearbeitung rechtmässig erfolgt.

Verweise: Art. 10a revDSG; BBI 2003 2135 f.

7. Meldepflicht (Art. 11a)

71 Müssen künftig auch Datensammlungen angemeldet werden, die bisher nicht meldepflichtig waren?

Mit der Revision wird die Meldepflicht grundsätzlich weiter gefasst, als dies bisher der Fall

war: Die Ausnahme von der Meldepflicht für diejenigen Fälle, in denen die Betroffenen über die Bearbeitung informiert sind, wird künftig nicht mehr gelten. Im Gegenzug wurden dafür generelle Ausnahmen von der Meldepflicht vorgesehen, wenn der Datenbearbeiter einen unabhängigen Datenschutzverantwortlichen einsetzt und dies dem EDÖB meldet sowie wenn der Datenbearbeiter eine Zertifizierung erlangt. Weiter wurden die in der Verordnung vorgesehenen Ausnahmen angepasst; nicht meldepflichtig sind nun z.B. Datensammlungen über Lieferanten und Kunden, soweit sie keine besonders schützenswerten Personendaten enthalten.

Bisher nicht meldepflichtige Datensammlungen müssen somit neu beim EDÖB gemeldet werden, wenn keiner der neu vorgesehenen Ausnahmefälle zutrifft. Für die Meldung dieser Datensammlungen wird der EDÖB den geltenden Art. 38 DSGVO analog anwenden und damit eine Frist von einem Jahr ab dem Inkrafttreten der Revision für die Meldung gewähren.

Verweise: Art. 11a revDSG; BBl 2003 2137 f.

72 Wer muss die Datensammlung anmelden, wenn die Datenbearbeitung durch Dritte erfolgt (Outsourcing)?

Zur Meldung verpflichtet ist der Inhaber der Datensammlung. Sofern keine Ausnahmegründe gegeben sind (vgl. oben, Ziff. 71), muss er die Datensammlung anmelden, auch wenn er die Bearbeitung nicht selbst vornimmt.

73 Gelten Mailsysteme sowie Protokolldateien (Logfiles) und Sicherungsdateien (Backups) als Datensammlungen, die angemeldet werden müssen?

Daten, die in elektronischen Kommunikationssystemen (z.B. E-Mail-Systeme) anfallen, sind grundsätzlich nicht als eigenständige Datensammlungen zu betrachten. In der Regel ist das elektronische Kommunikationssystem nur ein Übermittlungsinstrument und nicht ein Instrument zur strukturierten Verwaltung und Bearbeitung von Personendaten. Daher sind Datenbestände, wie sie in solchen Systemen anfallen, nicht meldepflichtig.

Für Protokolldateien (Logfiles) und archivierte Dateien, die nicht mehr operativ verwendet werden, sind in der Verordnung Ausnahmen von der Meldepflicht vorgesehen.

Sicherungsdateien (Backups) gelten nicht als eigenständige Datensammlungen und müssen nicht zusätzlich angemeldet werden.

74 Müssen auch Datensammlungen angemeldet werden, die eine Mitarbeiterin oder ein Mitarbeiter als persönliches Arbeitshilfsmittel benutzt?

Bestände an Personendaten, die als persönliches Hilfsmittel zur Auftragserfüllung im Arbeitsprozess dienen, sind grundsätzlich nicht meldepflichtig. Eine Meldepflicht ist namentlich dann nicht gegeben, wenn es sich dabei um Kopien von Daten handelt, die aus einer Datensammlung stammen, für die eine Meldepflicht gilt.

Als persönliche Arbeitshilfsmittel gelten Unterlagen oder in elektronischer Form gespeicherte Informationen dann, wenn sie nur vom Ersteller oder der Erstellerin oder einem eng begrenzten Personenkreis (bspw. neben dem Ersteller noch dessen Stellvertreter und seine Chefin) verwendet werden. Beispiele:

- Arbeitskopien von Korrespondenz, die ihrerseits in einem Kunden- oder Patientendossier abgelegt ist;
- persönliche Notizen zur Gedächtnisstütze über Kunden, die ein Mitarbeiter auf seinem PC oder in einem persönlichen Serververzeichnis anlegt.

Eine Anmeldung über Internet wird für die Privaten im Zeitpunkt des Inkrafttretens noch nicht möglich sein. Der EDÖB ist bemüht, das entsprechende System so schnell wie möglich zur Verfügung zu stellen.

8. Rechtfertigung der Bearbeitung (Art. 12 Abs. 2)

81 Welche Auswirkungen in der Praxis haben die Änderungen, die beim Mechanismus der Rechtfertigung der Bearbeitung vorgenommen wurden (Art. 12 Abs. 2 DSGVO)?

Der Gesetzgeber wollte mit der bei Art. 12 Abs. 2 DSGVO vorgenommenen Änderung nicht grundsätzlich vom heutigen System abweichen. Er wollte die Rechtfertigungsgründe bei Abweichungen von den allgemeinen Datenschutzgrundsätzen nicht generell ausschliessen, wohl aber:

- durch die textliche Änderung verdeutlichen, dass eine Rechtfertigung nicht vorschnell angenommen werden darf;
- Missverständnisse vermeiden bei Grundsätzen, bei denen kaum denkbar ist, dass ihre Verletzung zu rechtfertigen ist (insb. beim Grundsatz von Treu und Glauben bzw. der Rechtmässigkeit der Datenbearbeitung).

Hinweise zur Beurteilung der Rechtmässigkeit von Datenbearbeitungen nach der Neuerung:

- Vorliegen einer Einwilligung: Ist die Bearbeitung für die Betroffenen erkennbar (Art. 4 Abs. 4 revDSG) oder wurden sie hinreichend darüber informiert (Art. 7a revDSG) und entspricht die Einwilligung den Voraussetzungen nach Art. 4 Abs. 5 revDSG, so ist die darauf gestützte Datenbearbeitung zulässig.
- Überwiegende Interessen der Datenbearbeiter: Dass überwiegende Interessen der Datenbearbeiter bei der Beurteilung der Rechtmässigkeit zu berücksichtigen sind, ergibt sich bereits aus dem Verhältnismässigkeitsgrundsatz. Dieser verlangt – auch bei Datenbearbeitungen durch Private – die Prüfung von Geeignetheit, Erforderlichkeit sowie (im Rahmen der Prüfung des Verhältnisses von Bearbeitungszweck und –mitteln) die Abwägung der entgegengesetzten Interessen.
- Spezialgesetzlich geregelte Bearbeitung: Wenn eine spezialgesetzliche Rechtsgrundlage eine Bearbeitung von Personendaten vorsieht, so ist die Rechtmässigkeit der Bearbeitung weiterhin grundsätzlich gegeben. Das bringt schon der geltende Art. 4 Abs. 3 DSGVO zum Ausdruck, der bezüglich von Abweichungen vom Zweckbindungsgrundsatz spezialgesetzliche Bestimmungen vorbehält. Beispiele für solche spezialgesetzlichen Rechtsgrundlagen sind etwa die an Private gerichteten Mitteilungspflichten nach dem Konsumkreditgesetz¹, dem Epidemienengesetz² oder dem Geldwäschereigesetz³.

Zu dieser Thematik hat das BJK eine Auslegungshilfe verfasst, die auf weitere Einzelheiten eingeht. Sie ist auf dem Website des BJK abrufbar:

http://www.bj.admin.ch/etc/medialib/data/staat_buerger/gesetzgebung/datenschutz.Par.0019.File.tmp/20070111-Auslegungshilfe-d.pdf

¹ Art. 25 ff. Bundesgesetz über den Konsumkredit, SR 221.214.1

² Art. 27 Epidemienengesetz, SR 818.101

³ Art. 9 Geldwäschereigesetz, SR 955.0

9. Sperrung der Datenbearbeitung (Art. 15 Abs. 1 und 3)

91	Was ist mit dem Begriff der „Sperrung der Bearbeitung“ gemeint?
----	---

Der Begriff der Sperrung der Bearbeitung wird aus der Terminologie des EU-Rechts übernommen. Bei der Sperrung wird die Verfügung über die Daten nicht aufgegeben; die Nutzung wird indessen ganz oder teilweise eingeschränkt. Eine Sperrung kann somit – je nach den konkreten Umständen – für jegliche Bearbeitung (ausser dem Aufbewahren der Daten) oder auch bloss für einzelne Bearbeitungskategorien (etwa die Bekanntgabe an Dritte) verlangt werden.

BRU / 1.11.2007

R:\SVR\RSPM\Projekte\DSG Revision\Umsetzung revDSG_FAQ_def. Fassung 011107.doc