swissstaffing

Merkblatt: Revidiertes Bundesgesetz über den Datenschutz (revDSG)

Konsequenzen für Personaldienstleister in der Schweiz

1. Ausgangslage

Am 1. September 2023 tritt das totalrevidierte Bundesgesetz über den Datenschutz (Datenschutzgesetz; revDSG) zusammen mit der neuen Verordnung zum Datenschutz (DSV) sowie der neuen Zertifizierungsverordnung (VDSZ) in Kraft. Eine Übergangsfrist wird es nicht geben.

Mit Inkrafttreten des revDSG müssen Personaldienstleister neue Pflichten einhalten und entsprechende Massnahmen ergriffen haben. Nachfolgend sollen diese deshalb näher umschrieben werden. Die Verweise auf die jeweiligen Gesetzesbestimmungen beziehen sich dabei auf diejenigen des revidierten DSG (revDSG).

Das revDSG bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Personendaten (nachfolgend auch „Daten“ genannt) bearbeitet werden (Art. 1 revDSG). Es gilt für die Bearbeitung von Personendaten natürlicher Personen durch private Unternehmen und Bundesorgane (Art. 2 Abs. 1 revDSG).

Mit dem revDSG sollen mehrere Ziele verwirklicht werden:

- Die Schwächen des bestehenden DSG aus dem Jahre 1992, die aufgrund der rasanten technologischen Entwicklung entstanden sind, sollen behoben werden;
- Entwicklungen in der Europäischen Union soll Rechnung getragen und der Datenschutz in der Schweiz damit der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) angeglichen werden. Diese gilt seit dem 25. Mai 2018 (siehe swissstaffing Merkblatt vom Mai 2018). [Zu den Anpassungen für Unternehmen, welche bereits die Anforderungen an die EU-DSGVO umgesetzt haben, siehe im Anhang CHECKLISTE 1: VON DER EU-DSGVO ZUM REVDSG];
- Good Practices sollen gefördert werden, indem die Pflichten der für die Datenbearbeitungen verantwortlichen Personen erhöht und die Rechte der von einer Datenbearbeitung betroffenen Personen sowie die Aufsichtskompetenzen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gestärkt werden.

2. Was bleibt gleich mit Inkrafttreten des revidierten revDSG?

Unverändert bleiben im revDSG die Grundprinzipien der Datenbearbeitung. Es gilt deshalb weiterhin, dass wenn die nachfolgend aufgeführten Bearbeitungsgrundsätze eingehalten werden, für die Bearbeitung von Personendaten grundsätzlich weder eine Einwilligung noch ein Rechtfertigungsgrund erforderlich ist (Art. 6, 7 und 8 in Verbindung mit Art. 30 revDSG):

- Daten dürfen nur rechtmässig erhoben werden. Dies bedeutet, dass sie nicht durch Drohung oder Täuschung oder ohne das Wissen der Betroffenen beschafft werden dürfen (Art. 6 Abs. 1 revDSG).
- Die Bearbeitung der Daten nach Treu und Glauben zu erfolgen. Es gilt somit das Gebot des redlichen, vertrauenswürdigen und rücksichtsvollen Verhaltens (Art. 6 Abs. 2 revDSG).
- Der Grundsatz der Verhältnismässigkeit muss eingehalten werden. Dieser besagt, dass im einzelnen Fall zwar so viele Daten wie nötig, gleichzeitig aber so wenige wie möglich zu bearbeiten sind (Art. 6 Abs. 2 und 4 revDSG).

- Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein; der Zweck muss entweder bei der Beschaffung angegeben werden oder aus den Umständen ersichtlich sein (Art. 6 Abs. 3 revDSG).
- Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern (Art. 6 Abs. 5 revDSG).
- Die Datensicherheit muss gewährleistet sein; das heisst, Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 8 revDSG).

Eine Persönlichkeitsverletzung liegt – wie im bisherigen DSG – dann vor, wenn Personendaten bearbeitet werden, obschon einer der oben aufgezählten allgemeinen Grundsätze verletzt wird oder wenn die betroffene Person deren Bearbeitung ausdrücklich untersagt hat (Art. 30 Abs. 1 und 2 revDSG). Die Bearbeitung von Personendaten ist in diesen Fällen dennoch erlaubt, wenn ein Rechtfertigungsgrund gegeben ist. Rechtfertigungsgründe sind die Einwilligung der betroffenen Person, ein überwiegendes privates oder öffentliches Interesse oder ein Gesetz (Art. 31 Abs. 1 revDSG). Art. 31 Abs. 2 revDSG zählt Fälle auf, in denen ein überwiegendes privates Interesse der bearbeitenden Person (Verantwortlicher im Sinne des revDSG) gegeben sein kann.

Neben den allgemeinen Regelungen im revDSG ist die Bearbeitung von Personendaten für den Arbeitgeber in der Schweiz wie bisher auch in Art. 328b Obligationenrecht (OR) und für Personaldienstleister und -verleiher im Arbeitsvermittlungsgesetz (AVG) sowie in der Arbeitsvermittlungsverordnung (AVV) geregelt. Diese Bestimmungen konkretisieren vor allem den datenschutzrechtlichen Grundsatz der Verhältnismässigkeit (Art. 6 Abs. 2 revDSG). Es kann daher zur Bearbeitung von Personendaten im Personalkontext auf die bereits im Rahmen der EU-DSGVO erarbeiteten Klauseln verwiesen werden [siehe auch BEISPIEL 1: MUSTER EINWILLIGUNGSKLAUSEL und MUSTER 2 DATENSCHUTZ- UND EINWILLIGUNGSKLAUSEL IN AGB im Anhang dieses Merkblatts mit einem gemäss revDSG aktualisierten Muster]. Es sind insbesondere folgende Punkte zu beachten:

- Der Arbeitsvermittler- oder Verleiher darf Personendaten nur erfassen, soweit und solange sie für die Vermittlungs- und Verleihtätigkeit erforderlich sind (Art. 7 Abs. 3 und Art. 18 Abs. 3 AVG). Werden durch den Personaldienstleister Referenzen über Kandidaten eingeholt, erfordert dies die Einwilligung der betroffenen Person (Art. 47 Abs. 1 Buchst. b und Art. 19 Abs. 1 Buchst. b AVV).
- Die Bearbeitung der Bewerbung eines Kandidaten lässt sich durch ein überwiegendes privates Interesse des Arbeitsvermittlers- oder Verleihers an der Bearbeitung der Personendaten für die Prüfung der Bewerbung sowie für die Weitergabe an den entsprechenden Arbeitgeber bzw. Einsatzbetrieb rechtfertigten. Die Erhebung von weiteren Daten oder die Speicherung und spätere Verwendung der Bewerberdaten nach Abschluss des Anstellungsverfahrens bedürfen aufgrund der Zweckgebundenheit einer Einwilligung des Bewerbers.
- Nach Abschluss des Bewerbungsverfahrens sind die Bewerberdaten grundsätzlich zu löschen. Es dürfen nur noch die Vertragsgrundlagen für die Rechnungsstellung aufbewahrt werden, wofür eine gesetzliche Aufbewahrungsfrist von 10 Jahren besteht. Die weitere Aufbewahrung und damit ein Verzicht auf die Löschung des Personaldossiers oder die Weitergabe an andere potenzielle Arbeitgeber erfordert eine Einwilligung des Bewerbers.

In gewissen Fällen kann es zur Durchführung der Verleih- bzw. Vermittlertätigkeit erforderlich sein, besonders schützenswerte Personendaten (zum Beispiel Gesundheitsdaten) zu erfassen (siehe auch Ziff. 3.3 dieses Merkblatts). Werden besonders schützenswerte Personendaten durch den Bewerber mit den

Bewerbungsunterlagen mitgeteilt, dürfen diese nur im Rahmen der Bewerbung bearbeitet werden. Sollen diesen Daten weiterverwendet werden und ist eine Einwilligung des Bewerbers erforderlich ist, hat diese ausdrücklich zu erfolgen.

3. Welche Neuerungen bringt das revDSG?

3.1 Kein Schutz mehr von juristischen Personen

Geschützt sind nach revDSG nur noch die Daten natürlicher Personen, nicht mehr auch die Daten juristischer Personen wie etwa jene einer Aktiengesellschaft oder von Vereinen (vgl. Art. 2 revDSG). Diesen verbleiben der Schutz durch das Firmenrecht sowie der Persönlichkeitsschutz nach ZGB.

3.2 Neue Begriffe: Verantwortlicher und Auftragsbearbeiter

Statt wie bisher vom Inhaber einer Datensammlung zu sprechen, wird neu das Begriffspaar Verantwortlicher und Auftragsbearbeiter eingeführt. Verantwortliche sind private Unternehmen (juristische Personen), die allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung der Personendaten entscheiden (Art. 5 Buchst. j revDSG). Beim Personalverleih ist der Verleiher Verantwortlicher, gegebenenfalls zusammen mit dem zukünftigen Einsatzbetrieb. Der Verleiher ist als rechtlicher Arbeitgeber die erste Anlaufstelle des Arbeitnehmers und bearbeitet Personendaten für den Bewerbungsprozess. Findet sich ein passender Einsatzbetrieb, werden die Personendaten weitergeleitet, sodass der Einsatzbetrieb und der Verleiher zum Teil gleichzeitig die Personendaten bearbeiten und deshalb in diesem Moment beide Verantwortliche nach revDSG sind.

Nach Abschluss einer erfolgreichen Vermittlung bearbeitet der Arbeitgeber die Personendaten hingegen zukünftig jeweils zu eigenen Zwecken, weshalb er ab diesem Zeitpunkt alleiniger Verantwortlicher ist.

Auftragsbearbeiter sind private, in der Regel ebenfalls juristische Personen, die im Auftrag des Verantwortlichen Personendaten bearbeiten (Art. 5 Buchst. j revDSG). Beispiele hier sind etwa der IT-Dienstleister, an den – beruhend auf der Cloud-Technologie – der Personaldienstleister Datenbearbeitungen ausgelagert, oder Dienstleister, welche die Lohn- und Gehaltsabrechnungen von Mitarbeitern des Personaldienstleisters erstellen.

3.3 Erweiterung des Katalogs besonders schützenswerter Personendaten

Der Katalog der besonders schützenswerten Personendaten (etwa Gesundheitsdaten, politische Daten) wurde um biometrische und genetische Daten erweitert (Art. 5 Buchst. c revDSG). Für die Bearbeitung von besonders schützenswerten Personendaten gelten strengere Anforderungen als zur Bearbeitung von „normalen“ Personendaten. Bedarf es zu deren Bearbeitung einer Einwilligung der betroffenen Person, hat diese ausdrücklich zu erfolgen (Art. 6 Abs. 7 Buchst. a revDSG).

3.4 Profiling und Profiling mit hohem Risiko

Die technologische Entwicklung erlaubt es heute in immer stärkerem Ausmass, enorme Datenmengen automatisiert zu erfassen, zu bearbeiten, zu kombinieren und zu analysieren, um so beispielsweise Tendenzen, Korrelationen oder andere Merkmale feststellen zu können, die wiederum bestimmten Gruppen zugeordnet werden können. Unter Zuhilfenahme solcher Vergleichsgruppen lassen sich in der Folge Eigenschaften oder das Verhalten einzelner natürlicher Personen bestimmen bzw. vorhersagen, Neu wird deshalb im revDSG der Begriff des Profilings eingeführt. Dabei wird unterschieden zwischen „normalem“ Profiling und Profiling mit hohem Risiko. (Normales) Profiling ist jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte,

die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere, um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen (Art. 5 Buchst. f. revDSG). Ein solches normales Profiling liegt etwa dann vor, wenn ein Verkäufer alle Käufer von bestimmten Weinen, anschreibt, weil er glaubt, sie seien am ehesten an einer neuen Lieferung solcher Weine interessiert. Ein solches Verhalten schränkt die revDSG nicht mehr und nicht weniger ein als jede andere Datenbearbeitung auch.

Führt ein Profiling zu einer Verknüpfung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt, so handelt es sich um ein Profiling mit hohem Risiko. Eine solche Bearbeitung birgt ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person. Anwendungsbeispiele sind hier eine Bonitätsprüfung und Betrugsanalysen. Zukünftig dürften solche Bearbeitungen wohl auch in Bewerbungsprozessen vermehrt eine Rolle spielen. Bei Profiling mit hohem Risiko gelten strengere Voraussetzungen hinsichtlich der Personendatenbearbeitung. Sofern die Einwilligung der betroffenen Person erforderlich ist, hat diese ausdrücklich zu erfolgen (Art. 6 Abs. 7 Buchst. b revDSG). In der Regel muss auch eine sogenannte Datenschutz-Folgenabschätzung (DSFA) gemacht werden (vgl. Ziff. 3.11).

3.5 Data Protection by Design und Data Protection by Default

Nach dem im revDSG neu eingeführten Prinzip Data Protection by Design (Datenschutz durch Technik) ist der Verantwortliche verpflichtet, bei der Planung der Datenbearbeitung diese technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden (Art. 7 Abs. 1 und 2 revDSG). Mit anderen Worten ist eine Software und Hardware von Grund auf so zu konzipieren und zu entwickeln, dass sie die Grundsätze der Bearbeitung einhält (vgl. Ziff. 2 oben). Ferner hat der Verantwortliche nach dem Prinzip Data Protection by Default (datenschutzfreundliche Voreinstellungen) mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck notwendige Mindestmass beschränkt wird soweit die betroffene Person nicht etwas anderes bestimmt (Art. 7 Abs. 3 revDSG).

3.6 Flächendeckende Informationspflicht

Nach revDSG sind Informationen zur Bearbeitung der Personendaten den betroffenen Personen flächendeckend bereitzustellen (Art. 19 ff. revDSG). Datenschutzerklärungen auf Webseiten, Apps und Formularen sind Beispiele dafür, wo angegeben wird, wie die Personendaten konkret bearbeitet und wie die Informationen den betroffenen Personen bereitgestellt werden können. Mindestens folgende Informationen sind den Betroffenen zur Verfügung zu stellen:

- die Identität und die Kontaktdaten des Verantwortlichen;
- der Bearbeitungszweck;
- die Kategorien der bearbeiteten Personendaten (falls diese nicht bei der Person direkt beschafft werden);
- gegebenenfalls die Empfänger oder Kategorien von Empfängern, denen Personendaten bekannt gegeben werden; und
- die Länder, in welche die Personendaten übermittelt werden und auf welcher Rechtsgrundlage dies geschieht (etwaige vertragliche Garantien oder in Anspruch genommene Ausnahmen) [siehe hierzu Ziff. 3.9 sowie im Anhang CHECKLISTE 2: UMSETZUNG DER ANFORDERUNGEN AN DAS REVDSG].

3.7 Ausweitung der Betroffenenrechte

Nach revDSG bleiben die bisherigen Rechte der betroffenen Personen auf Auskunft, Löschung oder Sperrung (Einschränkung) ihrer Personendaten erhalten und werden teilweise angepasst. Betroffene Personen haben Anspruch auf alle Informationen, die erforderlich sind, um ihre Rechte geltend zu machen und eine transparente Datenbearbeitung zu gewährleisten (Art. 25 Abs. 2 revDSG). Die Auskunft ist grundsätzlich kostenlos und hat in der Regel innerhalb von 30 Tagen zu erfolgen (Art. 25 Abs. 6 und 7 revDSG). Neu eingeführt wird auch ein Recht auf Datenportabilität (Art. 28 ff. revDSG). Demnach kann jede Person von einem Verantwortlichen verlangen, sie betreffende und ihm vorgängig bekanntgegebene sowie auf Basis einer Einwilligung oder eines Vertrags automatisiert bearbeitete Personendaten in einem gängigen elektronischen Format herauszugeben oder diese Daten einem anderen Verantwortlichen zu übergeben (Art. 28 revDSG).

3.8 Vetorecht bei der Bearbeitung von Personendaten durch Auftragsbearbeiter

Nach revDSG kann das Bearbeiten von Personendaten durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn die Daten so bearbeitet werden, wie der Personaldienstleister selbst es tun dürfte und keine gesetzlichen oder vertraglichen Geheimhaltungspflichten bestehen, welche die Auslagerung verbieten (Art. 9 Abs. 1 revDSG). Beispiele für einer Übertragung der Bearbeitung von Personendaten an Dritte (Auftragnehmer) sind datenbearbeitungstechnische Arbeiten für die Lohn- und Gehaltsabrechnung, die Finanzbuchhaltung durch Rechenzentren, die auf der Cloud-Technologie beruhende Auslagerung der Datenbearbeitung an einen IT-Dienstleister oder der Einsatz von Dienstleistern zum Versand von Newslettern. Der Verantwortliche bleibt in diesen Fällen nach wie vor verantwortlich für die Datenbearbeitung. So muss er sicherstellen, dass der beauftragte Dritte die Datensicherheit gewährleistet (Art. 8 Abs. 2 revDSG). Neu darf der Auftragsbearbeiter die Bearbeitung erst mit vorgängiger Genehmigung des verantwortlichen Unternehmens einem Dritten übertragen (sogenanntes Vetorecht) (Art. 9 Abs. 3 revDSG). Allfällige Datensicherheitsverletzungen hat der Auftragsbearbeiter dem Verantwortlichen so rasch als möglich zu melden (Art. 24 Abs. 3 revDSG). Entsprechend empfiehlt es sich in einem Anhang zum entsprechenden Vertrag mit dem Dienstleister oder in den AGB eine Verpflichtung zur Einhaltung der datenschutzrechtlichen Pflichten zu formulieren. Ein Muster einer solchen Formulierung in den AGB ist im Anhang aufgeführt [BEISPIEL 3: MUSTER AUFTRAGSBEARBEITUNGSKLAUSEL IN DEN AGB].

3.9 Liste der Länder mit gleichwertigem Datenschutz publiziert durch den Bundesrat

Gemäss revDSG muss bei der Datenbekanntgabe ins Ausland - wie dies beispielsweise beim Einsatz eines Dienstleisters mit Sitz im Ausland (z.B. eines IT-Service Providers mit Sitz in den USA) der Fall ist - sichergestellt werden, dass die Persönlichkeit der betroffenen Personen nicht gefährdet wird. Die Datenübermittlung in Länder mit einem gleichwertigen Datenschutz und somit das Outsourcing an entsprechende ausländische Outsourcingnehmer ist ohne Weiteres zulässig (Art. 16 Abs. 1 revDSG). Die Länder mit gleichwertigem Datenschutz werden in einer Liste publiziert. Darunter fallen die Schweiz und auch alle EU-Länder. Neu wird die Liste der Länder mit gleichwertigem Datenschutz durch den Bundesrat und nicht mehr durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) publiziert.

Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten nur ins Ausland bekannt gegeben werden, wenn hinreichende Garantien, einen solchen Schutz gewährleisten (Art. 16 Abs. 2 revDSG). Solche hinreichenden Garantien sind insbesondere die Europäischen

Standardvertragsklauseln (SCC). Ausnahmen hierzu sind möglich, so unter anderem wenn die betroffene Person ausdrücklich in die Bekanntgabe eingewilligt hat (Art. 17 Abs. 1 Buchst. a revDSG).

3.10 Meldepflicht bei Datensicherheitsverletzungen

Bei Datenschutzverletzungen muss das verantwortliche Unternehmen dem EDÖB (und gegebenenfalls den betroffenen Personen) Verletzungen der Datensicherheit, welche voraussichtlich ein hohes Risiko für die betroffenen Personen darstellen, so rasch als möglich melden (Art. 24 Abs. 1 revDSG). Darunter fallen etwa die Entwendung, bzw. der Diebstahl von Personendaten durch interne oder externe Personen (zum Beispiel Hacker) oder die Zerstörung von Informationen, beispielsweise aufgrund von Benutzerfehlern, technischen Fehlern, Viren oder Angriffen durch Hacker. In der Regel dürfte die Meldung von der Geschäftsleitung veranlasst werden. Letztendlich sind allerdings die Mitglieder des Verwaltungsrates im Rahmen des Risikomanagements hierfür verantwortlich (vgl. Art. 754 Abs. 1 OR). Das verantwortliche Unternehmen muss die Verletzungen dokumentieren. Die Dokumentation muss die mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung mindestens zwei Jahre aufzubewahren (Art. 15 Abs. 4 DSV).

3.11 Neue formale Pflichten nach revDSG

Personaldienstleister haben schliesslich zukünftig formale Pflichten im Zusammenhang mit der Bearbeitung von Personendaten einzuhalten:

- Benennung einer zentralen Stelle für den Datenschutz (z.B. Rechtsdienst, IT).
- Ein Unternehmen mit mehr als 250 Mitarbeitenden muss ein Verzeichnis der Bearbeitungstätigkeiten von Personendaten führen (Art. 12 revDSG). Zu den 250 Mitarbeitenden sind auch temporäre Mitarbeitende zu zählen. In Ausnahmefällen müssen Unternehmen mit weniger als 250 Mitarbeitenden ebenfalls ein Verzeichnis führen, nämlich wenn sie besonders schützenswerte Personendaten in grossem Umfang bearbeiten oder Profiling mit hohem Risiko betreiben.

  Das Verzeichnis des Verantwortlichen muss mindestens die folgenden Angaben enthalten:
  - Identität des Verantwortlichen,
  - Bearbeitungszweck,
  - Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten,
  - Kategorien der Empfänger,
  - Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer,
  - Beschreibung der Datensicherheitsmassnahmen und
  - bei Auslandsbekanntgabe die Angabe des Staates sowie der Garantie, welche einen geeigneten Datenschutz gewährleistet.
- Der Personaldienstleister als Verantwortlicher im Sinne des revDSG muss technische und organisatorische Massnahmen für die Informationssicherheit umsetzen, um die Personendaten angemessen zu schützen (Art. 8 revDSG) (siehe hierzu den Link zum Leitfaden zu den technischen und organisatorischen Massnahmen mit Bezug auf das aktuelle DSG des EDÖB im Anhang: NÜTZLICHE LINKS).
- Das verantwortliche Unternehmen hat vorgängig eine Datenschutz-Folgenabschätzung (DSFA) zu erarbeiten, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen kann. Bei heikleren Vorhaben wie der Einführung besonderer Applikationen besteht demnach eine Pflicht, eine formalisierte Risikoanalyse durchzuführen und zu

dokumentieren. Wann ein hohes Risiko vorliegt, ergibt sich aus verschiedenen Umständen, so insbesondere aus der Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung der Personendaten. Die DSFA selbst enthält eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person und die in diesem Zusammenhang getroffenen Massnahmen zum Schutz der Persönlichkeit und der Grundrechte. Sie ist also im Wesentlichen eine Risikoanalyse (Art. 22 f. revDSG). Einige Kantone, so etwa der Kanton Zürich, haben Formulare zur Erarbeitung einer DSFA publiziert [siehe im Anhang: NÜTZLICHE LINKS].

- Schliesslich sind auch die Mitarbeitenden hinsichtlich des Datenschutzes zu sensibilisieren und zu schulen.

4. Sanktionen

Mit dem revDSG werden auch die Bussen wesentlich erhöht. Wer die nachfolgend aufgeführten Pflichten des revDSG vorsätzlich (inklusive eventualvorsätzliche Inkaufnahme des sanktionierten Verhaltens) verletzt, muss mit einem Bussgeld von bis zu 250'000 Franken rechnen (Art. 60 ff. revDSG) bei:

- falscher und unvollständiger Auskunft;
- Verletzung der Informationspflichten;
- Nichteinhaltung der Mindestanforderungen an die Datensicherheit;
- unzulässiger Auslandsübermittlung;
- Auftragsbearbeitung, welche nicht den gesetzlichen Vorgaben entspricht;
- Verletzung der Vertraulichkeitspflicht.

Dies führt dazu, dass nach revDSG Verantwortliche im Unternehmen wie CEOs, CFOs oder CIOs direkt sanktioniert werden können. Immerhin handelt es sich bei den meisten Strafbestimmungen um Antragsdelikte, ein Verstoss wird also nur verfolgt, wenn etwa eine betroffene Person einen Strafantrag stellt.

5. Handlungsbedarf für Schweizer Personaldienstleister

Nr. 1 **Prüfung Internetauftritt** (Datenschutzerklärung, AGB, Applikationen, Newsletter Versand, Einwilligungserklärungen)	**Nr. 2** **Prüfen / Abschluss von Verträgen bei Datenbearbeitungen durch Dritte (inkl. Datenübermittlung ins Ausland)** (Vertrag, Weisungsrecht, keine Verletzung der Geheimhaltungspflichten, Datensicherheit, Vetorecht, Meldepflicht bei Datenübermittlung ggf. angemessene Garantien)
Nr. 3 **Prüfen, ob die Datenschutzgrundsätze eingehalten werden** (Rechtmässigkeit, Treu und Glauben, Verhältnismässigkeit, Zweckbestimmung, Datenrichtigkeit, Datensicherheit)	**Nr. 4** **Erarbeitung Prozess für Meldung bei Datensicherheitsverletzung** (bei hohem Risiko an EDOB/betroffene Person)
Nr. 5 **Erarbeiten von Prozessen betr. Rechte von Betroffenen** (Auskunftsprozess, Berichtigungsprozess, Löschprozess, Widerspruchsprozess, Prozess für Datenportabilität)	**Nr. 6** **Einhaltung formaler Pflichten** (Zentrale Datenschutzstelle, Mitarbeiterschulung, Verzeichnis der Bearbeitungstätigkeiten ab 250 Mitarbeitenden DSFA)

Zum konkreten Handlungsbedarf für Personaldienstleister siehe auch im Anhang CHECKLISTE 2: UMSETZUNG DER ANFORDERUNGEN AN DAS REVDSG.

Für Fragen steht der Rechtsdienst von swissstaffing gerne zur Verfügung unter 044 / 388 95 75 oder legal@swissstaffing.ch.

Zürich, im März 2023

swissstaffing

CHECKLISTE 1: ANPASSUNGEN VON DER EU-DSGVO ZUM REVDSG

Sofern Sie bereits die Anforderungen an die EU-DSGVO umgesetzt haben, ermöglicht Ihnen diese Checkliste zu prüfen, welche Anpassungen im Hinblick auf das revDSG noch umzusetzen sind.

Wichtig: Es ist gut möglich, dass neben dem revDSG auch die EU-DSGVO zur Anwendung kommt, weshalb die Anforderungen gegebenenfalls parallel gelten.

<table>
<tr><td>Nr. 1</td><td>Anwendbarkeit des revDSG

Oftmals wird in den erarbeiteten Dokumenten nur auf die EU-DSGVO verwiesen. Neu ist dieser Verweis zu erweitern und auch das revDSG miteinzubeziehen.</td><td>Neben der Anwendung der EU-DSGVO wird auch auf die Anwendung des revDSG verwiesen.</td><td>☐</td></tr>
<tr><td>Nr. 2</td><td>Begrifflichkeiten

Die Begrifflichkeiten des revDSG sind im Vergleich zu denjenigen der EU-DSGVO leicht anders:

<table><tr><th>revDSG</th><th>EU-DSGVO</th></tr><tr><td>Bearbeitung</td><td>Verarbeitung</td></tr><tr><td>Personendaten</td><td>personenbezogene Daten</td></tr><tr><td>besonders schützenswerte Personendaten</td><td>besonderer Kategorien personenbezogener Daten</td></tr><tr><td>Datensicherheitsverletzung</td><td>Datenschutzverletzung</td></tr></table></td><td>In den Dokumenten wurden die folgenden Begriffe angepasst: Verarbeitung/Bearbeitung, personenbezogene Daten/Personendaten, besondere Kategorien von Daten/besonders schützenswerte Daten, Datenschutzverletzung/Datensicherheitsverletzung</td><td>☐</td></tr>
<tr><td>Nr. 3</td><td>Weitergehende Definition von besonders schützenswerten Daten

Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen und Daten über Massnahmen der sozialen Hilfe gelten nach revDSG als besonders schützenswerte Personendaten. Entsprechend ist hier, sofern erforderlich, die Einwilligung ausdrücklich einzuholen.</td><td>Soweit erforderlich wird bei der Bearbeitung von Daten über verwaltungs- und strafrechtliche Verfolgung oder Sanktionen und Daten über Massnahmen der sozialen Hilfe die Einwilligung ausdrücklich eingeholt.</td><td>☐</td></tr>
<tr><td>Nr. 4</td><td>Erfüllung der Informationspflichten

Die für die Schweiz geltenden Informationspflichten sehen gewisse Differenzierungen gegenüber der</td><td>Die Datenschutzerklärung wurde um das Zielland bei einem Datentransfer ins</td><td>☐</td></tr>
</table>

	EU-DSGVO vor. In der Datenschutzerklärung ist die Angabe des Ziellandes bei einem Datentransfer ins Ausland aufzuführen.	Ausland ergänzt.	
Nr. 5	**Verzeichnis der Bearbeitungstätigkeiten** Im Verzeichnis der Bearbeitungstätigkeiten nach revDSG ist das Zielland anzugeben, sofern die Personendaten ins Ausland übermittelt werden sollen.	Das Verzeichnis der Bearbeitungstätigkeiten wurde um die Angabe eines Ziellands der Datenbearbeitung ergänzt.	☐
Nr. 6	**Prozess Datensicherheitsverletzung** Unter der EU-DSGVO sind sogenannte Datenschutzverletzungen mit einem Risiko für die betroffenen Personen innerhalb von 72 Stunden zu melden (Datendiebstahl und Datenmissbrauch). Unter dem revDSG ist eine Verletzung der Datensicherheit so rasch als möglich dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zu melden, sofern sie ein hohes Risiko für die betroffenen Personen mit sich bringt. Die Risikoschwelle, die eine Meldepflicht an die Datenschutzbehörde und/oder die betroffenen Personen auslöst, wird damit im revDSG anders definiert als in der EU-DSGVO.	Die Frist der Meldepflicht wurde von 72 h auf «so rasch als möglich» abgeändert und die Risikoschwelle angepasst.	☐
Nr. 7	**Prozess Gesuch betroffene Personen** Im Gegensatz zur EU-DSGVO enthält das revDSG neben Mindestinformationen, welche in jedem Fall einer betroffenen, auskunftsersuchenden Person zur Verfügung gestellt werden müssen, eine allgemeine Regelung, dass eine betroffene Person diejenigen Informationen erhält, die erforderlich sind, damit sie ihre Rechte geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist.	Der Prozess für Gesuche von betroffenen Personen wurde um die Möglichkeit ergänzt, dass eine betroffene Person, diejenigen Informationen erhält, die erforderlich sind, damit sie ihre Rechte geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist.	☐
Nr. 8	**Protokollierungspflicht** Im Unterschied zur EU-DSGVO kennt das revDSG	Sofern besonders schützenswerte Personendaten in	☐

	keine allgemeine "Rechenschaftspflicht". Im Zusammenhang mit der Datensicherheit gelten für die Bearbeitung von besonders schützenswerten Personendaten im grossen Umfang und für die Durchführung eines Profilings mit hohem Risiko allerdings umfassendere Pflichten als nach EU-DSGVO, wenn die präventiven Massnahmen den Datenschutz nicht gewährleisten. Demnach gilt für das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten von Daten eine Protokollierungspflicht und es muss ein Bearbeitungsreglement mit Angaben zur internen Organisation, zum Datenbearbeitungs- und Kontrollverfahren sowie zu den Massnahmen zur Gewährleistung der Datensicherheit erstellt werden. (Art. 4 Abs. 1 neueDSV). Eine Protokollierung muss insbesondere auch dann erfolgen, wenn sonst nachträglich nicht festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie beschafft oder bekanntgegeben wurden.	grossem Umfang automatisiert bearbeitet werden oder ein Profiling mit hohem Risiko durchgeführt wird und die präventiven Massnahmen den Datenschutz nicht gewährleisten, werden die Vorgaben an die Protokollierung eingehalten.	

swissstaffing

CHECKLISTE 2: UMSETZUNG DER ANFORDERUNGEN AN DAS REVDSG

Diese Checkliste ermöglicht es Ihnen, die Anforderungen an das revDSG umzusetzen und Ihren Status quo zu prüfen.

Nr. 1	**Prüfung des Internetsauftritts** Ihre Website ist Ihr Aushängeschild. Sie ist frei und öffentlich zugänglich. Die Datenschutzerklärung informiert über die Bearbeitung von Personendaten und erfüllt somit die Anforderungen an die Informationspflicht nach revDSG.	Die Datenschutzerklärung ist korrekt, vollständig und aktuell.	☐
		Die Datenschutzerklärung ist an gut sichtbarer Stelle auf der Webseite platziert.	☐
		Sofern die Webseite in mehreren Sprachen abrufbar ist, wurde die Datenschutzerklärung in die jeweiligen Sprachen übersetzt.	☐
		Sofern Allgemeine Geschäftsbedingungen (AGB) vorhanden sind, wurden sie auf Datenschutzkonformität geprüft.	☐
		Sofern ein Newsletter verschickt wird, wurde er auf Datenschutzkonformität geprüft.	☐
Nr. 2	**Prüfen/Abschluss von Verträgen bei Datenbearbeitungen durch Dritte (inkl. Thematik Datenübermittlung ins Ausland)** Beispiele: Verträge mit IT-Dienstleistern betr. der auf der Cloud-Technologie beruhenden Auslagerung von Datenbearbeitungen oder Verträge mit Dienstleistern für die Erstellung von Lohn- und Gehaltsabrechnungen von Mitarbeitern des Personaldienstleisters. Nach revDSG kann das Bearbeiten von Personendaten durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn die Daten so bearbeitet werden, wie der Personaldienstleister selbst es tun dürfte und keine gesetzlichen oder vertraglichen Geheimhaltungspflichten bestehen, welche die Auslagerung	Die Verträge mit den Dienstleistern wurden auf Datenschutzkonformität geprüft.	☐
		Es sind EU-Standardvertragsklauseln mit einem Dienstleister in einem Land ohne angemessenes Datenschutzniveau oder andere geeignete Garantien vereinbart und gegebenenfalls zusätzliche Massnahmen getroffen worden.	☐

	verbieten. Zudem muss das auftraggebende Unternehmen sicherstellen, dass der beauftragte Dritte die Datensicherheit gewährleistet (Art. 9 Abs. 1 und 2 revDSG). Neu darf der Auftragsbearbeiter die Bearbeitung erst mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen (Vetorecht) (Art. 9 Abs. 3 revDSG). Allfällige Datensicherheitsverletzungen hat der Auftragsbearbeiter dem Verantwortlichen so rasch als möglich zu melden (24 Abs. 3 revDSG). Der Personaldienstleister (Outsourcinggeber) bleibt verantwortlich für die Datenbearbeitung. Bei der Datenbekanntgabe ins Ausland muss sichergestellt werden, dass die Persönlichkeit der betroffenen Personen nicht gefährdet wird.		
Nr. 3	**Prüfen, ob die Datenschutzgrundsätze eingehalten werden** Es sind dies die Rechtsmässigkeit, die Zweckbindung, Treu und Glauben, die Verhältnismässigkeit und die Datenrichtigkeit, ggf. die Einwilligung, Datensicherheit, Privacy by Design und Privacy by Default.	Die Einhaltung der Grundsätze bei der Bearbeitung von Personendaten wurde geprüft.	☐
		Die Anforderungen an die Datensicherheit sind gewährleistet.	☐
		Es wurde geprüft, wo eine Einwilligung erforderlich ist und gegebenenfalls sichergestellt, dass diese erteilt wird.	☐
		Den Prinzipien Privacy by Design und Privacy by Default wird angemessen Rechnung getragen.	☐
Nr. 4	**Erarbeiten eines Meldeprozesses bei Datensicherheitsverletzungen**	Es wurde ein Prozess erarbeitet, wie im Falle eines Datensicherheitsvorfalls so rasch als möglich zu reagieren ist und wie der Vorfall dem Eidgenössischen Datenschutz und Öffentlichkeits-beauftragten (EDÖB) gemeldet und gegebenenfalls die betroffenen Personen	☐

		informiert werden können.	
Nr. 5	**Erarbeiten entsprechender Prozesse bei Gesuchen von betroffenen Personen**	Es existiert ein Prozess, wie im Falle von Gesuchen von betroffenen Personen vorzugehen ist, sodass die betroffene Person diejenigen Informationen erhält, die erforderlich sind, damit sie ihre Rechte geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Die Information ist ihr in der Regel innerhalb von 30 Tagen zu erteilen.	☐
Nr. 6	**Einhalten von formalen Pflichten**	Eine zentrale Anlaufstelle für alle datenschutzrechtlichen Fragen wurde benannt (z.B. Rechtsdienst, IT), gegebenenfalls wurde ein Datenschutzberater nach Art. 10 revDSG benannt, wobei letzterer über die erforderlichen Fachkenntnisse verfügen muss. Ferner muss er fachlich unabhängig und weisungsungebunden gegenüber dem Verantwortlichen sein und darf keine Tätigkeit ausüben, die mit seinen Aufgaben unvereinbar sind.	☐
		Sofern erforderlich, wurde ein Verzeichnis der Bearbeitungstätigkeiten erarbeitet.	☐
		Sofern erforderlich, wurde eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt.	☐
		Die Mitarbeitenden sind im Hinblick auf die Anforderungen an das revDSG sowie die im Unternehmen getroffenen Massnahmen geschult worden.	☐
		Sofern besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet werden oder ein Profiling mit hohem Risiko durchgeführt wird und die präventiven Massnahmen den Datenschutz nicht gewährleisten, werden die Vorgaben an die Protokollierung eingehalten.	☐

swissstaffing

BEISPIEL 1: MUSTER EINWILLIGUNGSKLAUSEL

[*Dieses Muster ist unvollständig und beispielhaft und ist auf den jeweiligen Einzelfall anzupassen*]

Die Bewerbungsunterlagen werden durch uns streng vertraulich behandelt und nur zum vereinbarten Zweck verwendet.

- Personalvermittlung: Die Daten werden nur soweit und solange bearbeitet, wie es für die Vermittlung erforderlich ist. Die Daten dürfen an mögliche Arbeitgeber weitergegeben werden.
- Personalverleih: Die Daten werden bis zur Beendigung des Verleihverhältnisses bearbeitet und Profile dürfen an (potentielle) Einsatzbetriebe weitergegeben werden.

Ohne Ihre Einwilligung wird das (elektronische) Bewerbungsdossier nach dem Abschluss des Bewerbungsverfahrens gelöscht/vernichtet, soweit es nicht einer gesetzlichen Aufbewahrungspflicht unterliegt.

Ich willige hiermit ausdrücklich in die nachfolgende Bearbeitung, Speicherung oder Übermittlung meiner Personendaten ein:

☐ Ich willige ein, dass [Personaldienstleister] meine Personendaten, die ich im Zusammenhang mit meiner Bewerbung mitgeteilt habe, innerhalb der Gesellschaften der [Personaldienstleister] im In- und Ausland [sofern kein angemessener Datenschutz: Angabe des Landes] zum Zwecke des Personalverleihs und/oder der Personalvermittlung gespeichert, bearbeitet oder übermittelt werden dürfen.

☐ Ich willige ein, dass meine Personendaten, die ich im Zusammenhang mit meiner Bewerbung mitgeteilt habe, während des Verleih- bzw. Vermittlungsverfahrens und über das Ende des konkreten Verleih- bzw. Vermittlungsverfahrens hinaus gespeichert, bearbeitet und an Dritte im In- und Ausland zum Zwecke des Personalverleihs und/oder der Personalvermittlung bekannt gegeben werden dürfen. Bei diesen Dritten handelt es sich unter anderem um mit [Personaldienstleister] verbundene Gesellschaften, Dienstleister, welche eingesetzte IT-Applikationen zur Verfügung stellen und betreiben, sowie weitere Unternehmen, welche an notwendigen Vorgängen der Erbringung der Vertragsleistungen von [Personaldienstleister] beteiligt sind (z.B. Zahlungsdienstleister). Insofern willige ich ein, dass meine Daten auch in Länder [Angabe des Landes] übermittelt werden, in denen kein angemessenes Datenschutzniveau besteht. Sofern ich im Zusammenhang mit meiner Bewerbung besonders schützenswerte Personendaten nach Art. 5 Buchst. c revDSG mitgeteilt habe (z. B. ein Foto, das die ethnische Herkunft erkennen lässt, usw.), bezieht sich meine Einwilligung auch auf diese Daten.

☐ Ich willige ein, dass [Personaldienstleister] Newsletter an die von mir angegebene E-Mail-Adresse senden lässt. Diese Newsletter enthalten insbesondere Informationen über Stellenangebote, die für mich interessant sein könnten.

Die Einwilligungen sind unabhängig voneinander und erfolgen freiwillig. Ich kann meine Einwilligungen jederzeit ohne Angabe von Gründen widerrufen und habe das Recht, jederzeit die Löschung meiner Personendaten zu verlangen. Über den Link am Ende jedes Newsletters kann ich mich von diesem abmelden. Ich nehme zur Kenntnis, dass im Falle eines Widerrufs meiner Einwilligungen zur Bearbeitung meiner Personendaten (mit Ausnahme der Einwilligung in den Erhalt des E-Mail-Newsletters) die von [Personaldienstleister] angebotenen Leistungen nicht weiter erbracht werden können und zu einer Beendigung der zugrundeliegenden Vertragsbeziehungen führen.

swissstaffing

BEISPIEL 2: MUSTER DATENSCHUTZ- UND EINWILLIGUNGSKLAUSEL IN DEN AGB

[*Dieses Muster ist unvollständig und beispielhaft und ist auf den jeweiligen Einzelfall anzupassen*]

Datenschutz

Die Parteien verpflichten sich, die einschlägigen Vorschriften zum Datenschutz jederzeit einzuhalten. Im Rahmen des jeweiligen Vertrags ist [Personaldienstleister] berechtigt, die Daten der Mitarbeiter, Geschäftsführer und sonstigen Angestellten des Kunden (nachfolgende „Personendaten" des Kunden) zu erheben, zu bearbeiten und zu allen mit der Vertragserfüllung zusammenhängenden Zwecken zu nutzen und offenzulegen. Hierzu gehört insbesondere auch die zur Vertragserfüllung unter Umständen notwendige Übermittlung von Personendaten des Kunden zu vorgenannten Zwecken ins Ausland [sofern kein angemessener Datenschutz: Angabe des Landes]. Zudem wird [Personaldienstleister] ausdrücklich ermächtigt, Personendaten des Kunden in jeder Form zu bearbeiten und an allfällige Konzerngesellschaften oder Dritte im Ausland bekannt geben zu dürfen.

Hiermit erteilt der Kunde die Einwilligung zur Nutzung der Personendaten des Kunden für Marketingzwecke. Der Kunde erklärt ausdrücklich, dass diese Einwilligung der betroffenen Personen vorliegt. [Personaldienstleister] kann diese jederzeit vom Kunden verlangen.

swissstaffing

BEISPIEL 3: MUSTER AUFTRAGSBEARBEITUNGSKLAUSEL IN DEN AGB

[*Dieses Muster ist unvollständig und beispielhaft und auf den jeweiligen Einzelfall anzupassen*]

Bearbeitung von Personendaten durch Dritte (Auftragsbearbeitung)

Der Auftragnehmer verpflichtet sich, an ihn weitergegebene oder ihm zugängliche Personendaten aus dem Bereich des [Personaldienstleisters] nur in dem Umfang und ausschliesslich zu denjenigen Zwecken zu bearbeiten, wie dies für die Vertragserfüllung notwendig ist.

Der Auftragnehmer verpflichtet sich, angemessene technische und organisatorische Massnahmen zur Gewährleistung des Datenschutzes und der Informationssicherheit zu treffen.

Der Auftragnehmer bearbeitet Personendaten (inkl. Zugriffe und Standort-Webserver) nur in der Schweiz oder in der EU, bzw. im Europäischen Wirtschaftsraum.

Der Auftragnehmer legt bereits vor Abschluss des Vertrages mindestens diejenigen Unterbeauftragten offen, die in seinem Auftrag Personendaten bearbeiten. Er überbindet allen involvierten Unterbeauftragten, Erfüllungsgehilfen und Dritten die Pflichten aus diesem Auftragsbearbeitungsvertrag. Für den Beizug jedes zusätzlichen Unterbeauftragten holt der Auftragnehmer von [Personaldienstleister] jeweils vorgängig die schriftliche Zustimmung ein. Solange die schriftliche Zustimmung nicht vorliegt, darf der Auftragnehmer keinen weiteren Unterbeauftragten einsetzen. Es liegt im alleinigen Ermessen des Auftraggebers, einen Dritten als zukünftigen Unterbeauftragten anzunehmen oder abzulehnen.

Der Auftragnehmer behandelt alle Personendaten, die er direkt oder indirekt im Zusammenhang mit dem Vertrag erlangt, vertraulich. Er sichert [Personaldienstleister] insbesondere zu, die Personendaten weder an unautorisierte Dritte weiterzugeben noch in anderer Form unautorisierten Dritten zugänglich zu machen. Die Verpflichtung zur Einhaltung der Vertraulichkeit überbindet der Auftragnehmer allen involvierten Unterbeauftragten, Erfüllungsgehilfen und Dritten.

Der Auftragnehmer unterstützt [Personaldienstleister] bei der Einhaltung der Anforderungen der anwendbaren Datenschutzbestimmungen. Insbesondere beantwortet er unverzüglich und ordnungsgemäss alle Anfragen des Auftraggebers im Zusammenhang mit der Bearbeitung von Personendaten. Begehren betroffener Personen oder Behörden leitet er unverzüglich [Personaldienstleister] weiter, ohne diese selber zu beantworten. Der Auftragnehmer ist verpflichtet, in allfälligen aufsichtsrechtlichen Verfahren, welche die von ihm zu erbringenden Leistungen betreffen, mitzuwirken und von ihm verlangte Auskünfte und Unterlagen zur Verfügung zu stellen.

Der Auftragnehmer informiert unverzüglich [Personaldienstleister] wenn er Kenntnis oder einen Verdacht hat, dass Personendaten, welche er für [Personaldienstleister] bearbeitet, einem unautorisierten Zugriff ausgesetzt, an unbefugte Dritte weitergegeben, verloren gegangen oder beschädigt worden sind oder in sonstiger Weise rechts- oder vertragswidrig bearbeitet wurden oder werden könnten. Der Auftragnehmer hat zudem umgehend diejenigen Sofortmassnahmen zu ergreifen, die erforderlich sind, um die Personendaten zu sichern und mögliche nachteilige Folgen zu verhindern bzw. zu minimieren.

[Personaldienstleister] hat das Recht, jederzeit die Einhaltung der anwendbaren Datenschutzbestimmungen beim Auftragnehmer zu kontrollieren.

Bei Vertragsbeendigung hat der Auftragnehmer die Personendaten (samt allfälliger Kopien), welche er für [Personaldienstleister] bearbeitet hat, vorbehältlich einer anderen Regelung im Vertrag, nach ausdrücklicher Anweisung des [Personaldienstleisters] an diesen zu übertragen oder zu vernichten. Die Datenvernichtung ist vom Auftragnehmer zu dokumentieren und eine Kopie dieser Dokumentation [Personaldienstleister] unaufgefordert zuzustellen.

ANHANG: NÜTZLICHE LINKS

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, das Dokument finden Sie hier

Medienmitteilungen des Bundesamtes für Justiz finden Sie hier und hier

Allgemeine Webseite des Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) finden Sie hier

Leitfaden zu den technischen und organisatorischen Massnahmen (2015) des EDÖB finden Sie hier

Formular zur Erstellung einer Datenschutz-Folgenabschätzung des Kanton Zürichs finden Sie hier