Adrian Bieri
Dr. iur., Rechtsanwalt, Partner
Leiter Practice Group Immaterialgüter,
Technologie und Datenschutz
Telefon +41 58 258 10 00
adrian.bieri@bratschi.ch

Die Totalrevision des schweizerischen Datenschutzgesetzes – was sind die wichtigsten Neuerungen und was müssen Unternehmen für die Umsetzung tun?

Am 25. September 2020 haben National- und Ständerat das totalrevidierte Bundesgesetz über den Datenschutz («nDSG») angenommen. Die Inkraftsetzung ist zwar erst im Jahr 2022 zu erwarten. Unternehmen sind jedoch gut beraten, die erforderlichen Anpassungen frühzeitig anzugehen. Der vorliegende Beitrag soll erstens eine konzise Darstellung der wesentlichen Neuerungen des neuen Datenschutzgesetzes liefern. Zweitens verschafft eine Checkliste zum Schluss des Beitrages einen Überblick über die wichtigsten Umsetzungsmassnahmen.

1. Wichtigste Neuerungen auf einen Blick

Zunächst ist festzuhalten, dass die Schweizer Datenschutzordnung trotz der Totalrevision des geltenden Bundesgesetzes über den Datenschutz («DSG») in ihren **wesentlichen Grundsätzen unverändert** bleiben wird. Eine Revolution hat daher, entgegen manchen Behauptungen, nicht stattgefunden.

Die Hauptziele der Revision bestanden in einer Anhebung des Datenschutzniveaus auf dasjenige in der europäischen Union gemäss der Datenschutz-Grundverordnung («DSGVO»), der Schaffung von mehr Transparenz bei der Bearbeitung von Personendaten und dem Ausbau der Rechte betroffener Personen.

Diesen Zielen entsprechend betreffen die wichtigsten Neuerungen für private Unternehmen zusammengefasst folgende Punkte:

- Die Informationspflicht bei der Beschaffung von Personendaten wurde erweitert und gilt neu grundsätzlich bei sämtlichen beabsichtigten Personendatenbeschaffungen (vgl. dazu unten Ziff. 2);
- Unternehmen müssen neu ein sog. Bearbeitungsverzeichnis führen, in welchem sie ihre Personendatenbearbeitungsaktivitäten zusammenfassen (vgl. dazu unten Ziff. 3);
- Unternehmen sind neu verpflichtet, mit ihren Auftragsbearbeitern eine Auftragsbearbeitungsvereinbarung abzuschliessen (vgl. dazu unten Ziff. 4);
- Die Datensicherheitsanforderungen wurden erhöht, indem Unternehmen neu (i) bestimmte Verletzungen der Datensicherheit dem EDÖB melden und (ii) im Vorfeld bestimmter Personendatenbearbeitungen eine sog. Datenschutz-Folgenabschätzung («DSFA») vornehmen müssen (vgl. dazu unten Ziff. 5);
- Die Betroffenenrechte wurden ausgebaut, insbesondere durch schärfere Sanktionen und das neu geschaffene Datenportabilitätsrecht (vgl. dazu unten Ziff. 6);
- Die im Datenschutzgesetz vorgesehene berufliche Schweigepflicht wurde erheblich erweitert (vgl. dazu unten Ziff. 7);
- Es wurden neue Strafbestimmungen bei Verstössen gegen das Datenschutzgesetz mit Bussen von bis zu CHF 250'000.00 eingeführt. Die neuen Bussen sind ad personam ausgestaltet worden und treffen daher die für ein Unternehmen tätigen natürlichen Personen, insbesondere Leitungspersonen (vgl. dazu unten Ziff. 8).

2. Erweiterte Informationspflicht bei der Beschaffung von Personendaten

Auch unter dem geltenden DSG besteht bereits eine Informationspflicht, wobei sich diese auf das Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen beschränkt. Mit dem revidierten Datenschutzgesetz wird diese **Informationspflicht grundsätzlich** auf **alle beabsichtigten Beschaffungen von Personendaten** ausgebaut. Im Rahmen dieser erweiterten Informationspflichten müssen Unternehmen den von einer Datenbearbeitung betroffenen Personen vor der Datenbeschaffung mindestens offenlegen, (i) welches Unternehmen der Verantwortliche für die Datenbearbeitung ist (inkl. Angabe der Kontaktdaten) und (ii) für welche Bearbeitungszwecke die Personendaten erhoben werden. Sofern ein Unternehmen beabsichtigt, die erhobenen Personendaten an Empfänger weiterzugeben, muss das Unternehmen offenlegen, (iii) an welche Empfänger bzw. an welche Kategorien von Empfängern die Personendaten bekanntgegeben werden (vgl. Art. 19 nDSG). Falls ein Unternehmen auch plant, die erhobenen Personendaten ins Ausland bekannt zu geben, müssen zusätzlich die Staaten genannt werden, in welche die Personendaten übermittelt werden. Erfolgt die Übermittlung in einen Staat ohne angemessenen Datenschutz, so müssen Unternehmen zusätzlich offenlegen, mit welchen Mitteln

(z.B. Abschluss von Standarddatenschutzklauseln für crossborder-data-transfers) sie einen angemessenen Datenschutz sicherstellen.

Zwar sieht das Gesetz auch **gewisse Ausnahmen** von **und Relativierungen** der Informationspflicht vor (vgl. Art. 20 nDSG). Gleichwohl werden die allermeisten Unternehmen in ihren Datenbearbeitungen davon betroffen sein bzw. inskünftig mehr informieren müssen.

Eine praktikable Umsetzung dieser datenschutzrechtlichen Informationspflicht kann über Datenschutzbestimmungen in AGB oder – besser – in den bereits weit verbreiteten **Online-Datenschutzerklärungen** («privacy policies») erfolgen. Da im heutigen Wirtschaftsleben im Verkehr mit Konsumenten die eigene Homepage sozusagen zum Gesicht des Unternehmens geworden ist, sind die dort enthaltenen Datenschutzbestimmungen besonders aussenwirksam (aber gleichzeitig auch für Behörden einsehbar), weshalb sichergestellt werden sollte, dass diese Datenschutzerklärungen auch mit den neuen Vorgaben des nDSG übereinstimmen.

Obschon insbesondere seit der Inkraftsetzung der DSGVO mannigfaltige Vorlagen und Muster für entsprechende Datenschutzerklärungen im Internet zirkulieren, ist von einer pauschalen Übernahme hiervon abzuraten. Solche Muster decken in der Regel nur Personendatenbearbeitungen ab, die über die Webseite erfolgen, nicht aber andere Personendatenbearbeitungen eines Unternehmens, über welche die Unternehmen gemäss der neuen Informationspflicht nun informieren müssen. Wichtig ist zudem, dass die Datenschutzerklärung die konkreten Datenbearbeitungen eines Unternehmens abbildet, was gewisse **Individualisierungsarbeiten** unumgänglich macht. Für viele Datenbearbeitungen werden aber auch kurze Datenschutz- oder – treffender – Datenbearbeitungserklärungen genügen, bei welchen sich Unternehmen mit ein paar wenigen Sätzen auf die Mindestangaben gemäss Art. 19 nDSG beschränken. Hier werden sich Unternehmen durchaus am Grundsatz **"weniger ist mehr"** ausrichten können.

3. Einführung eines Verzeichnisses über die Bearbeitungstätigkeiten («Bearbeitungsverzeichnis»)

Zu den neuen formellen Pflichten für Unternehmen gehört auch das Führen eines **Verzeichnisses über die Datenbearbeitungstätigkeiten** (Art. 12 nDSG; auch Bearbeitungsverzeichnis genannt). Es handelt sich hierbei um eine Art interne Buchführung über die verschiedenen Datenbearbeitungsprozesse eines Unternehmens. Während die Datenschutzerklärung vor allem gegen Aussen über die Datenbearbeitungen eines Unternehmens informiert, soll das Verarbeitungsverzeichnis eine interne Übersicht über die wichtigsten beabsichtigten Personendatenbearbeitungen beinhalten. Das Bearbeitungsverzeichnis soll Aufschluss über die Eckdaten im Zusammenhang mit den Bearbeitungsprozessen geben. Darunter fallen weitgehend die gleichen Angaben, die auch von der Informationspflicht nach Art. 19 nDSG erfasst werden. Für KMU ist indessen zu erwarten, dass der Bundesrat auf dem Verordnungsweg noch gewisse Erleichterungen zu dieser Pflicht erlassen könnte (vgl. Art. 12 Abs. 5 nDSG).

Angaben, die ein Bearbeitungsverzeichnis enthalten soll:

- Identität des Verantwortlichen;
- Bearbeitungszweck;
- Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten;
- die Kategorien der Empfängerinnen und Empfänger;
- wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;
- Angaben zu Bekanntgaben von Personendaten ins Ausland.

4. Neue Pflicht zum Abschluss von Auftragsbearbeitungsvereinbarungen

Wenn Unternehmen für eine Datenbearbeitung einen Auftragsbearbeiter einsetzen, muss der Verantwortliche neu aktiv sicherstellen, dass der Auftragsbearbeiter die Daten nur so bearbeitet, wie der Verantwortliche es selbst tun dürfte (vgl. Art. 9 nDSG). Das bedeutet konkret, dass der Verantwortliche den Auftragsbearbeiter darauf verpflichtet, die Personendaten ausschliesslich zum Zweck der Auftragsbearbeitung zu bearbeiten und ihn zur Einhaltung der datenschutzrechtlichen Grundsätze verpflichtet. Zur Umsetzung dieser Pflicht empfiehlt sich für Verantwortliche, mit ihren Auftragsbearbeitern eine **schriftliche Auftragsbearbeitungsvereinbarung** abzuschliessen.

Bevor Unternehmen jedoch Auftragsbearbeitungsvereinbarungen mit Dritten abschliessen, ist zunächst zu prüfen, ob überhaupt ein Auftragsbearbeitungsverhältnis im Sinne des Datenschutzrechts vorliegt. Die Datenschutzgesetzgebung kennt nämlich **verschiedene datenschutzrechtliche Rollen**, die den an einer Datenbearbeitung beteiligten Akteuren zufallen können. Mit jeder datenschutzrechtlichen Rolle sind unterschiedliche Rechte und Pflichten verknüpft, weshalb eine korrekte Eruierung der zutreffenden datenschutzrechtlichen Rolle für Unternehmen essenziell ist.

Die grundsätzliche Unterscheidung betrifft jene zwischen der datenschutzrechtlichen Rolle als Verantwortlicher (Controller) und derjenigen als Auftragsbearbeiter («Processor»). **Verantwortlicher** ist diejenige Person, die **über den Zweck und die Mittel der Datenbearbeitung (mit-)bestimmt** (Art. 5 lit. J nDSG). Die arbeitsteilige Wirtschaft von heute bedingt regelmässig den Einbezug von externen Dienstleistern zur effektiven Aufgabenerfüllung. Bearbeitet ein Dienstleister **im Auftrag eines Verantwortlichen** Personendaten, so gilt er nach dem nDSG grundsätzlich als **Auftragsbearbeiter** (Art. 5 lit. K nDSG). Diese Umschreibung vermag die Komplexität der Differenzierung im Einzelfall jedoch nicht vollständig wiederzugeben. In der Regel kann aus einem Auftragsverhältnis allein nicht automatisch auf eine Auftragsbearbeitung geschlossen werden. Gefordert wird, dass der **Schwerpunkt des Auftragsverhältnisses gerade in der Bearbeitung von Personendaten** liegt. Somit scheiden eine Vielzahl von Auftragsnehmern im vertragsrechtlichen Sinn als Auftragsbearbeiter im datenschutzrechtlichen Sinn aus (regelmässig etwa Anwälte oder

Banken), weil die Datenbearbeitung nur ein Mittel zur Auftragserfüllung darstellt, nicht aber den eigentlichen Auftragszweck.

Neben der Konstellation einer Datenbekanntgabe vom Controller an einen Auftragsbearbeiter sind daher auch Konstellationen möglich, in denen Personendaten **zwischen gemeinsam Verantwortlichen** ausgetauscht werden oder **zwischen eigenständigen Verantwortlichen**. Bei der Konstellation der gemeinsam Verantwortlichen entscheiden mehrere rechtlich voneinander unabhängige Unternehmen **gemeinsam** über einen einzigen Datenbearbeitungsprozess. Beim Austausch zwischen eigenständigen Verantwortlichen legt jedes beteiligte Unternehmen selbst fest, mit welchen Mitteln oder zu welchem Zweck die ausgetauschten Personendaten bearbeitet werden.

Die **Abgrenzung** ist in der Praxis **oftmals schwierig**, aber relevant, weil etwa nach der DSGVO die gemeinsam Verantwortlichen u.a. einer solidarischen Haftung für Datenschutzverletzungen unterliegen.

Beispiele Verantwortlicher:

- Anwalt, Steuerberater, Revisor, Bank bei Bearbeitung eines Zahlungsauftrages, Personalvermittlung, Zahlungsdienstleister für elektronische Zahlungen, Inkassounternehmen bei Forderungsübertragung, Reisebüro, beauftragte Warenzusendung wie etwa Weinversand – insbesondere, weil diese Dienstleister über die wesentlichen Parameter der Bearbeitung selbständig entscheiden und die Datenbearbeitung bloss Mittel zur Auftragserfüllung, nicht aber der eigentliche Auftragszweck ist.
- Social Media Plattformen, Betreiber einer Fitness-App – insbesondere, aufgrund der Datennutzung für eigene Marketing- und Analysezwecke.

Beispiele Auftragsbearbeiter:

- Cloud-Betreiber
- Externer IT-Support- oder Wartungsdienst
- Externe Lohnbuchhaltung

5. Neue Meldepflicht bei Verletzungen der Datensicherheit und Pflicht zur Erstellung von Datenschutz-Folgenabschätzungen («DSFA»)

Neu unterliegen Unternehmen einer **Meldepflicht** an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten («EDÖB») in Bezug auf festgestellte **Verletzungen der Datensicherheit**, sofern anzunehmen ist, dass diese Datensicherheitsverletzung «zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führ[en]» (Art. 24 Abs. 1 nDSG). Gemäss der Legaldefinition sind Verletzungen der Datensicherheit Vorgänge, bei denen «Personendaten verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden» (Art. 5 lit. H nDSG). Dabei ist irrelevant, ob die Verletzung

absichtlich oder widerrechtlich herbeigeführt worden ist. Auch genügt bereits die blosse Möglichkeit, dass Personendaten Unbefugten offengelegt worden sind, ohne dass dies nachweislich stattgefunden haben muss. Liegt eine solche Datensicherheitsverletzung vor, muss die Meldung an den EDÖB **so rasch als möglich erfolgen**. Der Gesetzgeber hat aber bei der Revision des Datenschutzgesetzes – im Gegensatz zur Regelung unter der DSGVO – davon abgesehen, eine bestimmte Meldefrist vorzusehen.

Beispiele:

- Einem HR-Mitarbeiter kommt ein USB-Stick mit diversen Daten über Arbeitnehmer abhanden.
- Server fallen einem Hackerangriff zum Opfer.
- Ein Mitarbeiter überträgt Daten über Endkunden in eine private Cloud mit Servern in den USA.
- Ein Angestellter sendet eine E-Mail mit Personendaten irrtümlicherweise an den falschen Empfänger.
- Ein Virus bringt die IT-Infrastruktur zum Erliegen und führt zur unwiderruflichen Vernichtung von Personendaten.
- Aufgrund eines Brandes werden Personalakten, von welchen keine Kopien vorhanden sind, zerstört.

Will ein Unternehmen eine neue Datenbearbeitung einführen – zu denken ist etwa an die Einführung einer neuen Mobile-App, das Einsetzen eines Tracking-Tools, das Betreiben einer Online-Plattform oder den Einsatz einer Videoüberwachungskamera – so schreibt das nDSG neu die Durchführung einer **Datenschutz-Folgenabschätzung** vor (kurz «DSFA»; Data Protection Impact Assessment, «DPIA»; Art. 22 nDSG). Dadurch sollen insbesondere die Grundsätze der Verhältnismässigkeit und der Datenminimierung verwirklicht und sichergestellt werden, dass die beabsichtigte Datenbearbeitung von Beginn weg an Prinzipien von «**privacy by design**» und «**privacy by default**» ausgerichtet ist (vgl. Art. 7 nDSG). Zwar greift die Pflicht zur Vornahme einer DSFA nur, «wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann», allerdings wird die Ermittlung, ob überhaupt ein solches «hohes Risiko» vorliegt, regelmässig eine zumindest eingeschränkte DSFA voraussetzen. Der Gesetzgeber fordert, dass die DSFA noch im Entwicklungsstadium der geplanten Datenbearbeitung stattfindet, soll sie doch das Unternehmen über die Datenschutzrisiken sensibilisieren und konkret umsetzbare Massnahmen zu dessen Minimierung präsentieren.

6. Ausbau der Betroffenenrechte

Betroffenen Personen gewährt bereits das geltende DSG eine Reihe von Rechten gegenüber Verantwortlichen von Datenbearbeitungen. Diese Rechte haben mit der Revision keine allzu weitgehenden Änderungen erfahren. Allerdings sind den Betroffenenrechten mehr «Zähne» verliehen worden, indem die **Sanktionen für Verstösse ausgebaut** worden sind (siehe zu den Sanktionen Ziff. 8).

Hervorzuheben ist an dieser Stelle das **Auskunftsrecht** (Art. 25 nDSG). Dieses ermöglicht betroffenen Personen grundsätzlich, Auskunft über die sie betreffenden Datenbearbeitungen zu erhalten, und zwar grundsätzlich auf Kosten des Datenbearbeiters. Der Verantwortliche hat, falls er zur fraglichen Person Personendaten bearbeitet, u.a. über den Bearbeitungszweck, die Dauer der Bearbeitung oder die Kriterien zur Festlegung einer solchen, die Herkunft der Daten und die Empfänger bzw. die Kategorien der Empfänger sowie allenfalls über grenzüberschreitende Bekanntgaben Aufschluss zu geben. Die Auskunft kann insbesondere verweigert werden, wenn überwiegende Interessen dagegensprechen (Art. 26 nDSG). Zu denken ist v.a. an Geheimhaltungsinteressen im Zusammenhang mit Geschäftsgeheimnissen. Der Verantwortliche hat jedoch eine Interessensabwägung im Einzelfall vorzunehmen, die überwiegenden Interessen aufzuführen und seinen Entscheid zu begründen.

Neu aufgenommen worden ist das **Recht auf Datenherausgabe und -übertragung** (Art. 28 nDSG; auch **Datenportabilitätsrecht** genannt). Dieses gewährt betroffenen Personen einen Anspruch gegenüber dem Verantwortlichen auf Herausgabe der eigenen Personendaten bzw. auf deren Übertragung an einen anderen Verantwortlichen. Der Anspruch besteht dann, wenn die Daten automatisiert bearbeitet werden und die Rechtsgrundlage für die Bearbeitung entweder in der Einwilligung der betroffenen Person oder in einer vertraglichen Beziehung mit ihr besteht. Die Daten sind in einem gängigen elektronischen Format herauszugeben. Das Recht auf Datenportabilität stellt Unternehmen vor neue, teilweise aufwendige, Herausforderungen. Je nach Branche kann sich deshalb die Einführung von automatisierten Übertragungsprozessen aufdrängen. Das Datenportabilitätsrecht ist auch ein wichtiges Instrument dafür, dass Personen inskünftig über sog. Personal Data Wallets u.ä. ihre Personendaten monetisieren können, derweil die absolute Mehrheit der betroffenen Personen ihre grundsätzlich werthaltigen Personendaten heute noch kostenlos Dritten zur Verfügung stellt (z.B. durch das Akzeptieren von Cookies/Tracking-Tools zu Marketingzwecken auf Webseiten und Mobile-Apps).

7. Neue berufliche Schweigepflicht

Die bereits im geltenden DSG bestehende **berufliche Schweigepflicht** ist im Rahmen der Revision erheblich erweitert worden. Gilt die berufliche Schweigepflicht nach geltendem DSG nur für geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile, wurde diese Schweigepflicht nach revidiertem Datenschutzgesetz auf sämtliche geheimen Personendaten ausgedehnt, von denen jemand bei der Ausübung eines Berufes Kenntnis erlangt hat (vgl. Art. 62 nDSG). Durch die Ausdehnung des Anwendungsbereichs auf alle geheimen Personendaten wurde quasi ein Berufsgeheimnis für jedermann eingeführt.

8. Stärkung des EDÖB und Verschärfung der Sanktionen bei Verstössen gegen das Datenschutzgesetz

Die **Befugnisse** des EDÖB sind im nDSG **deutlich erweitert** worden. Er kann insbesondere gegen Private und Bundesorgane eine Untersuchung einleiten, sofern genügend Anzeichen für

eine Verletzung der Datenschutzvorschriften bestehen (Art. 49 Abs. 1 nDSG). Im Falle von Datenschutzverletzungen hat der EDÖB namentlich die Kompetenz, die Anpassung, die Unterbrechung oder den Abbruch der relevanten Datenbearbeitung und die Löschung von Personendaten zu verfügen (Art. 51 Abs. 1 nDSG). Ausserdem kann der EDÖB die Erteilung der Information nach Art. 019 und 21 nDSG anordnen (Art. 51 Abs. 3 Bst. C nDSG). Gegen Verfügungen des EDÖB steht der Rechtsweg an das Bundesverwaltungsgericht offen (Art. 32 ff. VGG).

Im Gegensatz zum geltenden Recht wurden ferner die Strafbestimmungen im nDSG verschärft. In Bezug auf die Informationspflicht gilt neu eine **Busse von bis zu CHF 250'000.00** bei vorsätzlicher Erteilung von falschen oder unvollständigen Informationen bzw. bei vorsätzlicher Unterlassung der Information (Art. 60 Abs. 1 nDSG). Die gleiche Strafandrohung besteht bei der Missachtung von Verfügungen des EDÖB (Art. 63 nDSG) sowie bei der falschen Auskunftserteilung ihm gegenüber im Rahmen einer Untersuchung (Art. 60 Abs. 2 nDSG). Zur Überraschung vieler richten sich Bussen wegen Verstössen gegen das neue Datenschutzgesetz nicht – wie etwa im Kartellrecht – gegen die betroffenen Unternehmen, sondern sind vom Gesetzgeber ad personam ausgestaltet worden und treffen daher die für ein Unternehmen tätigen natürlichen Personen, insbesondere Leitungspersonen (vgl. Art. 29 StGB und Art. 6 des Bundesgesetzes über das Verwaltungsstrafrecht).

9. Zum Verhältnis zwischen dem CH-DSG und der EU-DSGVO

Ein Hauptziel der Revisionsarbeiten bestand in der Annäherung des schweizerischen Datenschutzrechts an die europäische Datenschutzgesetzgebung, insbesondere an die DSGVO. **Viele der Standards** aus der DSGVO sind daher **im nDSG übernommen** worden, weshalb Unternehmen, die bereits heute die DSGVO erfüllen, im Hinblick auf das nDSG mit keinem allzu grossen Anpassungsbedarf konfrontiert sein werden.

Schweizer Unternehmen sind indessen gut beraten, zu prüfen, ob sie gegebenenfalls dem **extraterritorialen Anwendungsbereich** der DSGVO unterstehen, insbesondere weil sie etwa Waren oder Dienstleistungen gezielt an Personen in der EU anbieten (vgl. Art. 3 Abs. 2 lit. A DSGVO). Falls die DSGVO auf eine Teilmenge der Datenbearbeitungen eines Unternehmens zur Anwendung gelangt, ist zu ermitteln, ob eine unterschiedliche rechtliche Handhabung der verschiedenen Bearbeitungen jeweils nach nDSG und DSGVO überhaupt praktikabel ist oder, ob eine pauschale Beachtung der DSGVO vorteilhafter erscheint.

10. Checkliste Handlungsbedarf

Insbesondere aufgrund der empfindlichen neuen Sanktionen, welche das revidierte Datenschutzgesetz vorsieht, nicht zuletzt aber auch wegen der in der Öffentlichkeit stetig zunehmenden Sensibilisierung für das Thema Datenschutz und den damit verbundenen **Reputationsrisiken bei Datenschutzverletzungen**, ist eine sorgfältige Umsetzung der gesetzlichen Anforderungen für die

allermeisten Unternehmen unausweichlich geworden. Datenschutz ist heute zum wichtigen Bestandteil einer jeden «Good Governance» geworden.

Weil das Datenschutzrecht nach wie vor für viele ein nur schwer durchdringbarer rechtlicher Dschungel darstellt und um zu verhindern, dass man vor lauter Bäumen den Wald nicht mehr sieht, haben wir die nachfolgende **Checkliste** erstellt, welche (ohne Anspruch auf Vollständigkeit) eine einfache Auflistung der wichtigsten Handlungsschritte zur Umsetzung des revidierten schweizerischen Datenschutzgesetzes enthält:

1. Feststellung der Ausgangslage Erhebung der verschiedenen aktuellen Prozesse, bei denen Personendaten bearbeitet werden		
1.1	Von welchen Personen bearbeiten wir Personendaten?	
1.2	Welche Arten von Personendaten bearbeiten wir?	
1.3	Zu welchem Zweck werden die Personendaten bearbeitet?	
1.4	Welches sind mögliche Rechtfertigungsgründe für die Bearbeitung?	
1.5	Welche externen Dienstleister sind mit der Datenbearbeitung befasst?	
1.6	Welche datenschutzrechtlichen Rollen kommen den involvierten Personen zu?	siehe Ziff. 4
1.7	Wo genau werden die Personendaten gespeichert?	
1.8	Werden die Personendaten ins Ausland übermittelt?	
1.9	Falls die Daten ausserhalb der EU bekannt gegeben werden: mit welchen Mechanismen wird der angemessene Datenschutz gewährleistet?	

2. Prioritärer Handlungsbedarf Erarbeitung der erforderlichen Datenschutz-Dokumentation		
2.1	Erstellung oder Anpassung von Datenschutzerklärungen und anderen Informationsträgern zwecks Erfüllung der datenschutzrechtlichen Informationspflicht	siehe Ziff. 2
2.2	Anpassung von Datenschutzbestimmungen in AGB	siehe Ziff. 2
2.3	Erstellung oder Anpassung von Verträgen mit Auftragsbearbeitern, eigenständigen Verantwortlichen oder gemeinsamen Verantwortlichen.	siehe Ziff. 4
2.4	Erstellung von Verzeichnissen über die Bearbeitungstätigkeiten	siehe Ziff. 4
2.5	Erstellung von Standard-Vorlagen für die Meldung von Verletzungen der Datensicherheit	siehe Ziff. 5
2.6	Erstellung von Standard-Vorlagen für die Beantwortung von Auskunftsbegehren	siehe Ziff. 5
2.7	Evaluation und ggf. Anpassung von Mechanismen zur Gewährleistung eines angemessenen Datenschutzniveaus bei Übermittlungen in unsichere Drittstaaten	

3. Sekundärer Handlungsbedarf Festlegung der erforderlichen Datenschutz-Prozesse		
3.1	Bezeichnung einer für den Datenschutz und insbesondere für die Beantwortung von Auskunftsbegehren intern verantwortlichen Person (vgl. hierzu auch die Möglichkeit der freiwilligen Ernennung eines Datenschutzberaters gemäss Art. 10 nDSG)	
3.2	Festlegung des internen Meldeprozesses bezüglich Verletzungen der Datensicherheit	siehe Ziff. 5
3.3	Festlegung von Konzepten zur sicheren Aufbewahrung und Vernichtung von Personendaten	
3.4	Festlegung von Prozessen zur regelmässigen Nachführung und Aktualisierung der Datenschutz-Dokumentation	
3.5	Festlegung von Prozessen zur Umsetzung von Datenschutz-Folgenabschätzungen	siehe Ziff. 5
3.6	Festlegung eines Aufbewahrungskonzepts für Einwilligungserklärungen in Datenbearbeitungen	
3.7	Festlegung von Prozessen zur Erfüllung des Rechts auf Datenherausgabe und Datenübertragung (Datenportabilität)	siehe Ziff. 7
3.8	Festlegung von Prozessen zur Löschung von Personendaten	

Basel
Lange Gasse 15
Postfach
CH-4052 Basel
T +41 58 258 19 00
F +41 58 258 19 99
basel@bratschi.ch

Bern
Bollwerk 15
Postfach
CH-3001 Bern
T +41 58 258 16 00
F +41 58 258 16 99
bern@bratschi.ch

Genf
Rue du Général-Dufour 20
1204 Genf
T +41 58 258 13 00
F +41 58 258 17 99
geneve@bratschi.ch

Lausanne
Avenue Mon-Repos 14
Postfach 5507
CH-1002 Lausanne
T +41 58 258 17 00
T +41 58 258 17 99
lausanne@bratschi.ch

St. Gallen
Vadianstrasse 44
Postfach 262
CH-9001 St. Gallen
T +41 58 258 14 00
F +41 58 258 14 99
stgallen@bratschi.ch

Zug
Gubelstrasse 11
Postfach 7106
CH-6302 Zug
T +41 58 258 18 00
F +41 58 258 18 99
zug@bratschi.ch

Zürich
Bahnhofstrasse 70
Postfach
CH-8021 Zürich
T +41 58 258 10 00
F +41 58 258 10 99
zuerich@bratschi.ch