Datenschutz-Self-Assessment-Tool (DSAT)

Revidiertes DSG & DSGVO

DSAT.ch

Autor: David Rosenthal

Fachredaktion: David Rosenthal (david.rosenthal@homburger.ch), David Vasella (david.vasella@walderwyss.com)

Mitwirkende: Luca Dal Molin, Giulia Boccadoro, Katrina Frame, Manuel Mühlestein

Version: *6.01 – 29.6.2018 (Versionsstände der Formulare siehe www.dsat.ch)*

Hinweis: *Dieses Datenschutz-Self-Assessment-Tool wird kontinuierlich weiterentwickelt. Anregungen nimmt die Fachredaktion gerne entgegen. Der Inhalt wird ohne Gewähr für Richtigkeit und Vollständigkeit zur Verfügung gestellt und stellt weder Rechtsberatung dar noch ersetzt sie diese. Die Benutzung erfolgt auf eigenes Risiko.*

Vorwort

Das Datenschutzrecht wird derzeit grundlegend erneuert. Die Einführung der EU-Datenschutz-Grundverordnung (**DSGVO**) hat auch in der Schweiz in vielen Unternehmen bis auf höchste Managementstufe für grosse Aufmerksamkeit gesorgt. Gleichzeitig wird das Schweizer Datenschutzgesetz (**DSG**) revidiert und mit Strafsanktionen versehen. Der Handlungsbedarf liegt damit auf der Hand. Dennoch herrscht vielerorts eine gewisse Ratlosigkeit und Unsicherheit, wie die neuen Anforderungen am besten umzusetzen sind. Angesichts der rechtlichen, aber vor allem auch operationellen Komplexität dieser Aufgabe ist eine Konzentration auf das Wesentliche entscheidend.

Vor diesem Hintergrund entstand die Idee, das Wissen und die Erfahrung aus der Umsetzung von Datenschutz-Compliance-Projekten in kondensierter Form in ein Werkzeug zu giessen und Unternehmen und Beratern kostenlos zur Verfügung zu stellen. Daraus ging ein Set an Formularen hervor, die im Sinne einer Selbstdeklaration ausgefüllt werden können und dem Unternehmen dabei zeigen, wo es das neue Datenschutzrecht einhält und wo Handlungsbedarf besteht. Gleichzeitig kann das Unternehmen auf diese Weise seine Dokumentationspflichten erfüllen. Das kann mit oder ohne Experten gehen, auch wenn nach der 80:20-Regel für komplexere Konstellationen nach wie vor besonderes Fachwissen erforderlich sein wird.

Das Werkzeug wurde vom Autor zu grossen Teilen in Kundenprojekten entwickelt und erfolgreich zum Einsatz gebracht. Es war jedoch bald klar, dass es einen Beitrag zum Datenschutz in der Schweiz leisten kann und daher auf eine breitere Basis gestellt werden sollte. Aus diesem Grund haben wir uns als Fachredaktion zusammengetan, und aus diesem Grund wird es nicht als kommerzielles Produkt, sondern unter einer freien Lizenz zuhanden von Unternehmen, Behörden und Beratern kostenlos und neutral zur Verfügung gestellt.

Wir als Fachredaktion haben uns deshalb zum Ziel gesetzt, das Werkzeug weiterzuentwickeln, die erforderliche fachliche Qualität sicherzustellen und auf dem neusten Stand zu halten. Wir setzen es beide in unserer Beratung ein und lassen unsere Erkenntnisse darin einfliessen, würden uns aber über Anregungen anderer Experten und Nutzer freuen. Wir möchten allerdings darauf hinweisen, dass viele der Aussagen im Werkzeug eine persönliche Meinung wiedergeben, die nicht unbedingt von allen geteilt wird. Uns ist jedoch wichtig, dass die Compliance auch im Bereich des Datenschutzes vernünftig bleibt, d.h. mit einem pragmatischen und risikobasierten Ansatz betrieben wird. Perfektion kann für die Compliance keine Leitlinie sein. Nach unserer Erfahrung auch im Umgang mit den Aufsichtsbehörden ist entscheidend, dass ein Unternehmen sich mit den relevanten Fragen ernsthaft auseinandersetzt, auch wenn es nicht überall und immer alle Anforderungen erfüllen kann.

Im April 2018

David Rosenthal, Homburger AG
david.rosenthal@homburger.ch

David Vasella, Walder Wyss AG
david.vasella@walderwyss.com

Inhaltsverzeichnis

Formulare abrufbar unter www.dsat.ch

Vorab: Einführung, Anleitung zur Durchführung des Self-Assessments, Glossar

Farbcodierung: DSG | DSGVO

Einführung

Was ist DSAT?

DSAT besteht aus einem Satz von Formularen, der eine strukturierte Selbstbeurteilung der Datenschutz-Compliance eines Unternehmens erlaubt, d.h. die Überprüfung, inwieweit die Bestimmungen des Datenschutzes sowohl unter dem revidierten DSG als auch der DSGVO eingehalten sind. Es wurde mit folgenden Zielen entwickelt:

– **80:20 Regel**: DSAT deckt nicht alle Fälle und Aspekte ab, aber die breite Masse der Datenbearbeitungen in einem Unternehmen lassen sich damit erfassen und beurteilen, ebenso die grundsätzlichen Strukturen.

– **Prinzip Selbstdeklaration:** DSAT arbeitet nach dem Prinzip der Steuererklärung, d.h. die für eine Datenbearbeitung verantwortlichen Personen (*Business Owner*) nehmen eine Selbstdeklaration vor, für deren Richtigkeit und Vollständigkeit sie verantwortlich sind. Sie entscheiden dabei, wie weit sie dabei gehen wollen, müssen dafür aber auch geradestehen. Eine Datenbearbeitung lässt sich beispielsweise in 15–30 Minuten beurteilen, aber es können ebenso mehrere Stunden darin investiert werden. In der Praxis hat sich ein Schnitt von zwei Stunden pro Datenbearbeitung als Mittelwert herauskristallisiert. Wer das Formular durcharbeitet, wird aber ohnehin für den Datenschutz sensibilisiert.

– **Auch ohne Expertenwissen:** Die Formulare enthalten zwar viel Know-how, doch wer sie ausfüllt, muss zwar seine Datenbearbeitungen und sein Unternehmen gut kennen, braucht aber *kein* eigenes Datenschutzwissen. Er muss die auf seinen Fall zutreffenden Aussagen ankreuzen, die so formuliert wurden, dass sie auch ohne juristisches Wissen beantwortet werden können. DSAT sagt ihm dann, ob die Bearbeitung datenschutzkonform ist. Experten brauchen nach der 80:20 Regel nur in unklaren oder besonderen Fällen beigezogen zu werden. In der Praxis hat sich allerdings gezeigt, dass es am effizientesten und effektivsten ist, wenn die Formulare von einem Fachmann begleitet ausgefüllt werden.

– **Risikobasierte Entscheide:** In der Praxis kann das Datenschutzrecht nicht vollständig eingehalten werden. Wesentlich ist daher, dass ein Unternehmen sich der Datenschutzregeln bewusst ist und in vernünftigem Rahmen versucht, sich daran zu halten. DSAT trägt dem Rechnung, indem es auf die in der Praxis wesentlichen Anforderungen fokussiert, bewusst gewisse Unschärfen in Kauf nimmt, wo Ausführlichkeit in der Praxis nicht sinnvoll ist, und es den verantwortlichen Personen damit erlaubt, risikobasierte Entscheide zu treffen. Sie können so Aspekte, die nicht allen Vorgaben genau entsprechen, aber keine relevanten Risiken für die betroffenen Personen bergen, akzeptieren. Unternehmen werden so nicht gezwungen, grundsätzlich konforme Datenbearbeitung wegen wenig relevanten Ausnahmen als nicht rechtmässig einzustufen.

– **Massnahmen festlegen:** Mit DSAT können nicht nur Lücken im Datenschutz ermittelt werden. Es hilft auch, Massnahmen zu definieren, mit denen diese Lücken geschlossen werden können. Auch bietet DSAT die üblichen Handlungsmassnahmen vorgefertigt an. Es braucht nur angekreuzt und komplettiert zu werden.

– **Auto-Dokumentation:** DSAT liefert dem Unternehmen nicht nur Antworten, es dokumentiert zugleich die Datenschutzkonformität und erforderlichen Massnahmen. Damit kommt das Unternehmen ohne Zusatzaufwand auch seiner Rechenschaftspflicht (Prinzip der *Accountability*) nach.

Für wen ist DSAT gedacht?

DSAT ist in erster Linie für Schweizer Unternehmen gedacht. Die Unternehmensgrösse spielt an sich keine Rolle, d.h. es kann sowohl von einem KMU als auch im Grosskonzern eingesetzt werden. Inhaltlich deckt es sowohl die Anforderungen des revidierten DSG (derzeit im Stand des Entwurfs des Bundesrats) und der DSGVO (ohne nationale Sonderregelungen der einzelnen EU-Mitgliedsstaaten) ab. Ein Schweizer Konzern mit Niederlassungen im Ausland kann die Formulare aber ohne Weiteres auch für seine ausländischen Niederlassungen in der EU bzw. im EWR oder ausserhalb einsetzen.

Für jede Unternehmenseinheit (d.h. juristische Person) ist die Beurteilung gesondert vorzunehmen, da weder das DSG noch die DSGVO eine Konzernbetrachtung kennt. Verantwortlich daher ist jeweils das einzelne Unternehmen, auch bei konzernweiten Datenbearbeitungen, und zwar unabhängig davon, ob es als datenschutzrechtlich Verantwortlicher ("Controller") oder als Auftragsbearbeiter ("Processor") handelt; dafür sind jeweils eigene Formulare vorgesehen.

Warum kostet DSAT nichts?

In DSAT steckt zwar grosses Know-how, doch ist es uns, mir als Autor und David Vasella als meinem Kollegen der Fachredaktion, ein Anliegen, dass der Datenschutz in der Schweiz kosteneffizient und vor allem vernünftig betrieben werden kann. Ich als Autor habe daher seit je her mein Know-how breit geteilt und es hat mir nicht geschadet. Ich setze DSAT auch in unserer eigenen Arbeit ein, damit wir uns bei unseren Klienten auf die wesentlichen Punkte und Probleme konzentrieren können. Davon gibt es ohnehin genug, und sie sind viel spannender. Indem ich als Autor DSAT für breite Kreise zugänglich mache, erhoffen ich mir auch entsprechendes Feedback, um DSAT laufend zu verbessern. Aus diesem Grund arbeite ich auch mit meinem Kollegen David Vasella zusammen, der es ebenfalls für sich benutzt. DSAT entstand übrigens durch Zufall im Rahmen eines Mandats, in welchem sich ein nicht genanntes Unternehmen aus der Finanzbranche dafür entschied, die "Gap-Fit-Analyse" bei einer Vielzahl von Bearbeitungen auf der Basis einer Selbstdeklaration vorzunehmen.

Wofür ist DSAT nicht geeignet?

DSAT ist nicht geeignet für die Beurteilung von datenschutzrechtlich komplexen Datenbearbeitungen und Konstellationen (nicht zu verwechseln mit datenschutzrechtlich heiklen Datenbearbeitungen) sowie Fragen in unklaren Situationen und Grenzbereichen. Die vorgefertigten Antworten und Freitextfelder in den Formularen bieten zwar einen gewissen Spielraum, die Komplexität einer Datenbearbeitung abzubilden. Unter Umständen hilft es auch, eine Datenbearbeitung in mehrere Teile aufzuteilen und jeden Teil gesondert zu beurteilen (die Formulare erlauben dies). Doch die Formulare wollen und können nicht jeden Fall abdecken, sondern sind nach der 80:20 Regel auf Standardsituationen ausgerichtet. Es wird in manchen Betrieben Datenbearbeitungen geben, die individuell durch einen Experten beurteilt werden müssen, sei es, weil sie zu komplex sind, sei es, weil sie zu viele Risiken für betroffene Personen oder das Unternehmen bergen. DSAT kann jedoch auch in diesen Fällen wertvolle Hinweise auf die Problembereiche liefern. Müssen die im Betrieb verantwortlichen Stellen es durcharbeiten, führt es im Übrigen auch zu einer Sensibilisierung dieser Stellen und fördert damit das Verständnis für den Datenschutz.

DSAT deckt auch die nationalen Sonderregelungen zur DSGVO nicht ab. Die DSGVO sieht an 71 Stellen vor, dass die Mitgliedstaaten der EU (und des EWR) zusätzliche Regelungen erlassen können. Das können sowohl zusätzli-

che Anforderungen und Einschränkungen sein als auch nationale Erleichterungen. Insbesondere für die Bearbeitung von Daten von Mitarbeitern kennen einige EU-Mitgliedsstaaten abweichende Regelungen. Auch die Vorschriften für betriebliche Datenschutzbeauftragte sind in bestimmten Staaten (wie z.B. Deutschland) schärfer als in der DSGVO. Sie gelten in erster Linie für Unternehmen mit Sitz bzw. Niederlassungen in den betreffenden Staaten, aber da der nationale Gesetzgeber selbst definieren kann, wie weit seine Bestimmungen auch extraterritorial gelten, können sie auch auf Schweizer Unternehmen Anwendung finden. Die nationalen Aufsichtsbehörden sind gemäss DSGVO auch für ausländische Unternehmen zuständig, sofern diese Datenbearbeitungen vornehmen, die auf Personen mit Wohnsitz im betreffenden Staat ausgerichtet sind (Erwägungsgrund 122). Ob und inwieweit ein Risiko besteht, dass ein Schweizer Unternehmen von ausländischem, nationalen Datenschutzrecht betroffen ist, ist mit einem Experten zum jeweiligen Landesrecht zu klären.

Sparen wir Zeit mit DSAT?

Ja, aber nur auf den zweiten Blick. Auch das Prinzip Selbstdeklaration erfordert, dass sich jemand – die für die Datenbearbeitung verantwortliche Person – mit den Anforderungen des Datenschutzes auseinandersetzt, mehr oder weniger intensiv. Diese Person kann das jedoch tun, wenn sie Zeit hat; sie muss sich nicht, wie das üblich ist, von einem Datenschutzexperten befragen lassen, der dann die Beurteilung vornimmt. Der Vorgang wird dadurch effizienter, auch wenn es im Rahmen einer Selbstdeklaration etliche Fälle geben wird, in welchen eine Situation unklar ist und daher ein Experte beigezogen werden muss. Hinzu kommt, dass in einem Unternehmen selten eine Person über alle erforderlichen Informationen über eine bestimmte Datenbearbeitung verfügt, um alle Fragen in DSAT beantworten zu können. Sie wird sich somit ihrerseits mit anderen Personen im Betrieb absprechen müssen.

Manche Fragebögen sind enorm lang! Wieviel Zeit brauchen wir dafür?

Das stimmt, aber der Eindruck täuscht. Der Fragebogen ist nicht lang, weil er so viele Fragen hat, sondern weil die typischen Antworten bereits aufgeführt sind. Die Länge der Fragebögen macht auch deutlich, wie komplex die Materie ist, obwohl versucht wurde, die Dinge zu vereinfachen, wo dies mit gutem Gewissen möglich ist. Dafür können die Aussagen durch Kreuzchen einfach ausgewählt werden, was eine rasche Beantwortung ermöglicht. Die Erfahrung zeigt, dass den Fragebogen (insbesondere Formular E.1, das Kernstück) schnell ausfüllen kann, wer ihn mit seinen Standardantworten kennt (in 15–30 Minuten pro Datenbearbeitung im Falle von Formular E.1). Das setzt natürlich voraus, dass diese Person auch die jeweilige Datenbearbeitung in der nötigen Tiefe kennt. Letzteres ist in der Praxis das Hauptproblem. Die Erfahrung hat auch gezeigt, dass die meisten Leute mit den Standardantworten in den Formularen ohne Datenschutzwissen gut zurechtkommen (allerdings werden die Formulare diesbezüglich laufend aktualisiert und Feedbacks sind willkommen). Damit die Fragebögen möglichst rasch beantwortet werden können, sind die wichtigsten Antworten auf den längeren Fragebögen vorangestellt, so dass sie "kurz und bündig" beantwortet werden können. Nur wer sich nicht sicher ist oder wem die Antworten nicht geeignet erscheinen, muss in die Detailbeantwortung einsteigen. Wer zum ersten Mal mit dem Fragebogen arbeitet, sollte sich daher insbesondere für das Formular E.1 zwei bis drei Stunden Zeit nehmen, um ihn zu verstehen. Hier kann sich auch ein erstes gemeinsames Ausfüllen mit einem Experten lohnen, im Sinne eines Workshops.

An wen können wir uns mit unseren Fragen wenden?

Wenden Sie sich an den Experten Ihres Vertrauens. Das kann die interne Datenschutzstelle sein, wenn Sie eine solche haben, oder ein externer Daten-

schutzberater oder Anwalt, der mit der Materie vertraut ist. Sie müssen nicht zu uns kommen. Wir empfehlen unseren Klienten, ab einer gewissen Unternehmensgrösse mindestens eine Person mit solidem Datenschutz-Know-how intern aufzubauen. Das muss kein Jurist sein, sollte aber jemand sein, der Freude am Thema und ein gewisses Flair für Unternehmensorganisation, Governance und Compliance hat, denn die meisten Herausforderungen stellen sich in diesem Bereich, nicht bei den rein rechtlichen Fragen. Für letztere kann bei Bedarf immer noch ein externer Berater beigezogen werden. Sollten Sie beim Umgang mit den Formularen Fragen haben, zum Beispiel, wie eine bestimmte Situation im Formular abzubilden ist oder was eine bestimmte Aussage bedeutet, und haben Sie niemanden, den Sie fragen können, so können Sie sich gerne auch an uns wenden. Allerdings behalten wir uns vor, entsprechende Leistungen in Rechnung zu stellen (darauf werden wir Sie aber vorgängig hinweisen). Für Feedbacks und Verbesserungsvorschläge sind wir dankbar.

Wie wird DSAT weiterentwickelt?

DSAT wurde letztlich aus der Not geboren, erfreut sich aber einiger Beliebtheit. Es ist ein Anfang, und es soll im Laufe der Zeit weiterentwickelt werden, basierend auf den Erfahrungen der Praxis und der Rechtsentwicklung. Zum Zeitpunkt der Lancierung existieren auch noch nicht alle Formulare. Die Weiterentwicklung ist die Aufgabe von mir, David Rosenthal, als Autor von DSAT und meinem Kollegen David Vasella, der mit mir die Fachredaktion bildet. Wie sich DSAT entwickelt, wird sich zeigen. Dies wird von der Akzeptanz im Markt abhängen. Die ersten Reaktionen sind allerdings sehr vielversprechend; DSAT kommt bisher ausgezeichnet an. In einer ersten Phase wird es daher darum gehen, mit Feedbacks diverser Unternehmen die Praxistauglichkeit und fachliche Basis zu verbessern. Inzwischen haben wir aber auch begonnen, Vorlagen von datenschutzrechtlichen Dokumenten (als erstes eine Datenschutzerklärung) auf DSAT anzubieten, weil wir gemerkt haben, dass dies eine grosse Hilfe vor allem für kleinere Unternehmen ist. Geplant sind auch weitere Sprachversionen, allerdings sind wir hier auf fremde Hilfe angewiesen, da uns selbst die Kapazität dafür fehlt (erste Angebote liegen vor).

Wo bekomme ich DSAT und vor allem Updates?

Für DSAT wurde eine eigene Website eingerichtet (www.dsat.ch). Auf dieser Website sind die aktuellsten Fassungen der diversen Formulare abrufbar. Sie können sich mit einer E-Mail-Adresse eintragen lassen, um jeweils über die neusten Anpassungen informiert zu werden. Die Unterlagen sind unter einer freien Lizenz verfügbar, d.h. jeder kann sich die Formulare für seinen Gebrauch entsprechend den Lizenzbedingungen herunterladen und nutzen. Über die Websites können auch Anregungen und Wünsche für Anpassungen, Ergänzungen, etc. kommuniziert werden. Neue Versionen sind dem Autor bzw. der Fachredaktion vorbehalten.

Sind Anpassungen für das eigene Unternehmen möglich?

Unternehmensspezifische Anpassungen sind derzeit nicht vorgesehen, aber nach individueller Absprache möglich, sofern das Unternehmen einwilligt, dass die Anpassungen in den "Standard" frei übernommen werden. Denkbar ist auch, dass darauf spezialisierte Unternehmen eine elektronische, automatisierte Variante von DSAT anbieten (d.h. in Form einer Web-Applikation, App oder sonstigen Software-Lösung). Da dies nicht der Kompetenzbereich des Autors ist, sollen sich darum andere kümmern. Auch hier kann der Inhalt von DSAT kostenlos zur Verfügung gestellt werden, wenn gewisse Voraussetzungen erfüllt sind. Hierzu ist der Autor zu kontaktieren.

Anleitung zur Durchführung des Self-Assessments

Funktionsweise und allgemeine Hinweise

DSAT besteht aus einem Set von PDF-Formularen. Jedes Formular deckt **einen anderen Aspekt des Datenschutzrechts** ab; es können, müssen aber nicht alle Formulare bearbeitet werden. Gewisse Formulare müssen mehrfach ausgefüllt werden (z.B. für jede Datenbearbeitung im Unternehmen eins). Es gibt **zwei Formularsorten**: Die eine Sorte dient lediglich der Dokumentation (A.1, A.2, B.1, B.2, B.3), während andere der datenschutzrechtlichen Beurteilung *und* Dokumentation dienen (z.B. E.1, C.1, D.1).

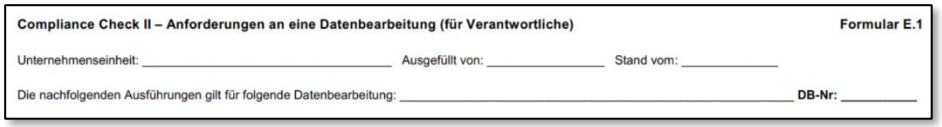
Der **Blickwinkel der Formulare** ist unterschiedlich:

– Solche, die sich auf das **gesamte Unternehmen** beziehen (A.1, A.2, B.1). Diese halten Basisinformationen fest, einschliesslich der Übersicht über alle Datenbearbeitungen.

– Solche, die für das gesamte Unternehmen oder auch nur für **spezifische Unternehmensbereiche** ausgefüllt werden können und dazu dienen, datenschutzrelevante Prozesse, Funktionen und Vorkehrungen zu beurteilen (z.B. D.1–5, F.1–3, C.1).

– Solche, die sich auf die **einzelnen Datenbearbeitungen** im Unternehmen beziehen (B.1–3, E.1–5, G.1, teilweise C.1). Diese bringen den grössten Aufwand mit sich, weil sie für jede Datenbearbeitung gesondert ausgefüllt werden müssen. Was eine "Datenbearbeitung" ist, wird später erläutert.

Auf der **ersten Seite jedes Formulars** kann jeweils angegeben werden, worauf sich das Formular bezieht (Unternehmenseinheit, Datenbearbeitung(en) mit Identifikationsnummer gemäss Formular B.1) sowie wann das Formular durch wen ausgefüllt wurde.


Compliance Check II – Anforderungen an eine Datenbearbeitung (für Verantwortliche) Formular E.1

Unternehmenseinheit: _____ Ausgefüllt von: _____ Stand vom: _____

Die nachfolgenden Ausführungen gilt für folgende Datenbearbeitung: _____ DB-Nr: _____

Jedes Formular ist so auszufüllen, dass es den *status quo* angibt, also **den momentanen Zustand**, und zwar auch dann, wenn der Zustand einer Datenbearbeitung oder die Situation im Unternehmen noch nicht datenschutzkonform ist und Massnahmen erst zu treffen sind. Sind diese getroffen, sollte das Formular erneut ausgefüllt werden. So kann der Fortschritt dokumentiert werden.

Alle Formulare sollten, sobald ausgefüllt, **archiviert** werden. Die **Dokumentation der Selbstbeurteilung** ist eine wichtige Funktion von DSAT und eine Anforderung des Datenschutzrechts (Prinzip der *Accountability*): Unternehmen müssen zeigen können, dass sie den Datenschutz einhalten, d.h. dass sie sich mit den Anforderungen des Datenschutzrechts auseinandergesetzt, ihre eigenen Datenbearbeitungen (und flankierenden Massnahmen) auf ihre Konformität hin beurteilt haben und, wenn nötig, Massnahmen zur Verbesserung identifiziert und ergriffen haben. Datenschutzbehörden können sich diese Dokumentation zeigen lassen.

Auf gewissen Formularen ist nicht nur anzugeben, wer sie ausgefüllt hat, sondern auch, wer **für die betreffende Datenbearbeitung verantwortlich** ist. Diese Person ist sowohl für das korrekte und vollständige Ausfüllen der

Selbstbeurteilung wie auch für die dabei getroffenen Entscheidungen betr. Konformität und etwaigen Massnahmen verantwortlich. Dies ist ein wichtiger Aspekt von DSAT: Jede für eine Datenbearbeitung verantwortliche Person muss für ihre Datenbearbeitung und deren Beurteilung **selbst die Verantwortung tragen**. Wenn sie sich in einem Punkt nicht sicher ist, muss sie von sich aus einen Experten oder die anderen nötigen Stellen fragen. Dies funktioniert wie bei der Steuererklärung: Wer nicht weiss, wie sie ausgefüllt werden muss, muss Hilfe holen.

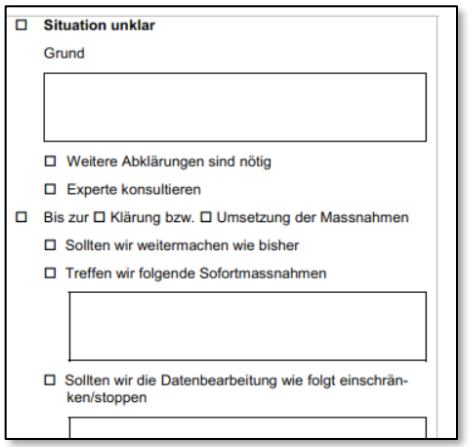
Am Ende des Formulars E.1 ist ferner eine Beurteilung durch die **Business Owner der von einer Datenbearbeitung betroffenen Prozesse** vorgesehen. In den meisten Unternehmen werden Datenbearbeitungen mit den Prozessen des Unternehmens nicht deckungsgleich sein. Da jedoch das **Risiko-Management** typischerweise an die Prozesse des Unternehmens anknüpft, wird mit dieser letzten Seite des Formulars E.1 die Brücke geschlagen und von den für die von einer Datenbearbeitung betroffenen Prozesse verantwortlichen Personen erfragt, ob sie damit verbundene Risiken zu tragen bereit sind oder aber welche Massnahmen umgesetzt werden müssen. Hierbei kann auch die **Ansicht der Datenschutzstelle**, sofern es eine solche gibt, festgehalten werden.

Das Formular E.1 und diverse weitere Formulare sehen vor, dass je nach Konformität des betreffenden Prozesses oder der betreffenden Datenbearbeitung bestimmte **Massnahmen zu treffen** sind. Diese sind als Vorschläge ausgestaltet, d.h. sie sind möglicherweise nicht alle sinnvoll oder nötig. Der **Entscheid über diese Massnahmen** und ggf. die Priorisierung und deckt DSAT *nicht* ab.

Sobald die Vorschläge für Massnahmen feststehen, empfehlen wir daher, die von den verantwortlichen Stellen vorgeschlagenen Massnahmen in ein **separates Dokument** (z.B. Excel) zu übernehmen, über die einzelnen Massnahmen zu entscheiden und sie zu priorisieren. In diesem separaten Dokument kann auch deren Umsetzung kontrolliert werden.

Sind die **Massnahmen** einer bestimmten Datenbearbeitung oder eines bestimmten Prozesses **vorgenommen**, kann das betreffende Formular, das dazu Anlass gab, erneut ausgefüllt werden, um den nun mehr datenschutzkonformen Zustand zu dokumentieren.

In den Beurteilungsformularen kann jeweils festgehalten werden, wenn die **Situation unklar** erscheint, d.h. der Beurteilungsvorgang nicht ohne zusätzliche Abklärungen oder Expertenunterstützung abgeschlossen werden kann. In diesen Fällen sind die betreffenden Abklärungen zu treffen bzw. Expertenmeinungen einzuholen.



Ebenfalls kann festgehalten werden, ob angesichts der Beurteilung **Sofortmassnahmen** erforderlich sind, bis hin zur vorübergehenden Einstellung einer Datenbearbeitung. Solche Sofortmassnahmen werden erfahrungsgemäss die absolute Ausnahme sein.

Der Ablauf

Der Ablauf der Selbstbeurteilung ist im nachfolgenden Flussdiagramm festgehalten. Die orangen Dokumente beurteilen einzelne Datenbearbeitungen, die blauen Dokumente übergreifende Prozesse, Funktionen oder Aspekte.

1. Begonnen wird mit **Formular A.1** und optional **Formular A.2**. Darin werden bestimmte Grundangaben zum Unternehmen festgehalten. Beurteilt wird noch nichts; die beiden Formulare dienen nur der Dokumentation. Es wird auch abgefragt, ob gewisse nach DSGVO teilweise erforderliche Stellen existieren. Ob es diese braucht, wird später mit Formular D.1 beurteilt.

   In einem Konzern ist für jede rechtliche Einheit (juristische Person) eine separate Beurteilung vorzunehmen. Die verschiedenen Gesellschaften eines Konzerns sind grundsätzlich wie Dritte zu behandeln, auch wenn sie z.B. bestimmte IT-Anwendungen (z.B. Personalverwaltung oder Buchhaltung) teilen. In diesen Fällen ist jede Unternehmenseinheit für ihren Teil der IT-Anwendung bzw. der darin verarbeiteten Daten verantwortlich.

2. In einem zweiten Schritt müssen die Datenbearbeitungen des Unternehmens ermittelt und in **Formular B.1** erfasst werden. Gemeint sind die verschiedenen Aktivitäten, in deren Rahmen *Personendaten* bearbeitet werden, also Information, die sich auf bestimmte oder bestimmbare natürliche Personen (d.h. Menschen) beziehen. Bestimmbar ist eine Person dann, wenn genügend Angaben vorliegen, anhand welcher die betroffene Person unter Zuhilfenahme anderer Datenquellen identifiziert werden kann, auch wenn dafür ein vertretbarer Zusatzaufwand betrieben werden muss (z.B. eine AHV-, Handy- oder eine Bankkonto-Nummer einer Person). Für den vorliegenden Kontext wird empfohlen, IP-Adressen und dauerhafte *Cookies* ebenfalls als Personendaten zu betrachten, auch wenn sie dies korrekterweise in manchen Fällen nicht sind (in der EU besteht jedoch eine starke Tendenz, sie als solche zu betrachten). Eine *Bearbeitung* ist jeder Umgang mit Personendaten, also solche erheben, nutzen, weitergeben oder auch nur aufbewahren.

   Es gibt keine bestimmte Regel, nach welchen Kriterien die Vielzahl an Datenbearbeitungen in einem Unternehmen aufzutrennen sind (nach IT-Anwendung, nach Geschäftsprozess, nach betroffenen Personen, nach verantwortlicher Person). Wesentlich ist, dass jene Aktivitäten zu einer Datenbearbeitung zusammengefasst und unter einem Titel und mit einer Nummer in Formular B.1 eingetragen werden, die eine logische Einheit bilden und für welche die Fragen insbesondere gemäss Formular E.1 bzw. Formular E.2 einheitlich beantwortet werden können. Die Zwecke von Q4 von Formular B.2 geben einen Hinweis auf typische Datenbearbeitungen, die alle Unternehmen haben (z.B. Personaladministration, Rekrutierung, Finanzen und Buchhaltung). Im Anhang von Formular B.1 ist – zur Inspiration – zudem das Beispiel einer Übersicht der Datenbearbeitungen eines mittelgrossen Unternehmens aufgeführt.

   Zu viele Datenbearbeitungen zu definieren, schafft unnötigen Aufwand. Ähnliche Datenbearbeitungsaktivitäten können und sollten daher zu einer Datenbearbeitung zusammengefasst werden, insbesondere, wenn dieselbe Person für sie verantwortlich ist und sie eine gewisse inhaltliche Einheit aufweisen (gleiche oder vergleichbare Zwecke, gleiches Risikoprofil, gleiche Art von Daten). In einem einfachen Unternehmen gibt es typischerweise ein- bis zwei Dutzend Datenbearbeitungen. Zwei Datenbearbeitungsaktivitäten sind dann in zwei verschiedene Datenbearbeitungen aufzutrennen und gesondert zu behandeln, wenn sich bei der datenschutzrechtlichen Beurteilung (d.h. Formular E.1 bzw. Formular E.2) zeigt,

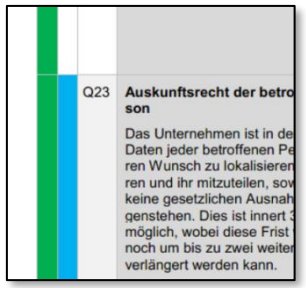
dass sie zu sehr unterschiedlichen Antworten führen und keine sinnvolle Beurteilung mehr möglich ist. Dafür gibt es keine scharfe Regel.

Die Aufteilung der Datenbearbeitungsaktivitäten in die einzelnen Datenbearbeitungen kann durchaus auch mit Bauchgefühl und ohne einheitliche Systematik vorgenommen werden. Entscheidend ist einzig, dass am Schluss alle wesentlichen Datenbearbeitungsaktivitäten beurteilt wurden und es nicht zu viele verschiedene Datenbearbeitungen gibt. Die Liste kann im Laufe der Zeit auch erweitert werden.

Im Formular B.1 ist für jede Datenbearbeitung auch festzuhalten, ob das Unternehmen als *Verantwortlicher* oder als *Auftragsbearbeiter* auftritt. Dort, wo das Unternehmen Daten für ein anderes Unternehmen (Kunde, andere Konzerngesellschaft) bearbeitet (z.B. für ein Outsourcing), ist das Unternehmen Auftragsbearbeiter. Dort, wo das Unternehmen selbst Herr der Daten ist und daher selbst bestimmt bzw. verantwortlich dafür ist, welche Daten wozu und wie bearbeitet werden, ist es Verantwortlicher.

Die Unterscheidung ist wichtig, weil das Unternehmen je nach Rolle unterschiedliche datenschutzrechtliche Pflichten hat. Bei diversen Formularen wird deshalb nach diesen beiden Rollen unterschieden. Die Rolle ist in Formular B.1 ebenfalls einzutragen, wobei im Falle einer Auftragsbearbeitung, alle vergleichbaren, für einen oder mehrere Kunden bzw. Konzerngesellschaften betriebenen Datenbearbeitungen zusammengefasst werden können (z.B. Server- und Anwendungsbetrieb für Konzerngesellschaften).

3. Im dritten Schritt wird ermittelt, inwieweit das revidierte DSG und die DSGVO auf die einzelnen Datenbearbeitungen Anwendung finden. Dazu dienen die beiden Fragen im **Formular C.1**. Bei einem Unternehmen in der Schweiz wird das DSG grundsätzlich immer Anwendung finden; trotzdem werden in Q1 die Voraussetzungen abgefragt, da das Formular auch für Unternehmen im Ausland eingesetzt werden kann, wo das revidierte DSG möglicherweise nicht zur Anwendung gelangt. In Q2 wird wiederum geprüft, ob und inwieweit die DSGVO zur Anwendung kommt. Hat das Unternehmen keine Niederlassung in der EU, so findet die DSGVO höchstens auf bestimmte Datenbearbeitungen Anwendung. Daher kann in Q1 und Q2 jeweils angegeben werden, für welche Datenbearbeitungen (von Formular B.1) welche Voraussetzungen erfüllt sind und daher das revidierte DSG bzw. die DSGVO gilt. Das Ergebnis sollte für jede Datenbearbeitung in Formular B.1 nachgetragen werden.



In allen anderen Formularen wird nach Anwendbarkeit des revidierten DSG und der DSGVO unterschieden. Die Anforderungen, die unter dem revidierten DSG zu beachten sind, sind mit einem grünen Balken markiert, jene, die im Rahmen der DSGVO zu beachten sind, mit einem blauen. Viele Anforderungen gelten für beide Gesetze. In Beurteilungsformularen wie Formular E.1 ist auf der Titelseite jeweils anzugeben, nach welchem Gesetz die betreffende Datenbearbeitung beurteilt wird.

4. Im vierten Schritt wird das gemäss DSGVO und revidiertem DSG erforderliche Verzeichnis der Datenbearbeitungen erstellt. Hierzu wird für jede Datenbearbeitung entweder das **Formular B.2** (wo das Unternehmen Verantwortlicher ist) und **Formular B.3** (wo das Unternehmen Auftragsbearbeiter ist) ausgefüllt. Es geht lediglich um eine Dokumentation der Datenbearbeitung; beurteilt werden sie dabei nicht. Die Formulare beschränken sich daher im Hinblick auf die Angaben auf das gesetzliche

Minimum. Es sind bereits zahlreiche Musterantworten enthalten. Diese beiden Formulare sind durch jene Stellen auszufüllen, die für die betreffenden Datenbearbeitungen verantwortlich sind. Dies sollte meist ohne fachliche Hilfe möglich sein.

5. Im fünften Schritt wird für jede Datenbearbeitung beurteilt, ob diese die Anforderungen des anwendbaren Datenschutzrechts (revidiertes DSG, DSGVO oder beide) erfüllen. Hierzu wird für jede Datenbearbeitung entweder das **Formular E.1** (wo das Unternehmen Verantwortlicher ist) und **Formular E.2** (wo das Unternehmen Auftragsbearbeiter ist) ausgefüllt. Dies ist der mit Abstand aufwändigste Schritt im Rahmen der Selbstbeurteilung. Auch hier sollten die Formulare durch jene Stellen ausgefüllt werden, die für die betreffenden Datenbearbeitungen verantwortlich sind. So wird der Aufwand im Unternehmen verteilt.

   Es ist ohne Weiteres möglich, dass ein Unternehmen sowohl Datenbearbeitungen in der Rolle als Verantwortlicher wie auch Datenbearbeitungen als Auftragsbearbeiter hat. In diesen Fällen muss das Unternehmen beide Formulare ausfüllen, jeweils für die entsprechenden Datenbearbeitungen.

   Die Formulare weisen mehrere Besonderheiten auf:

   – Jede Anforderung (beim Formular E.1 sind es 27) ist mit ein bis drei Kurzantworten versehen, welche die häufigsten Fälle zusammenfassen. Wenn eine solche Antwort genau passt, kann die Anforderung mit einem einzigen Kreuz beurteilt werden. Passen diese Kurzantworten nicht, oder ist die ausfüllende Person nicht sicher, so kann sie in die Detailantworten einsteigen.

   – Bei jeder Anforderung ist es das Ziel, in der mittleren Spalte (die den momentanen Zustand angibt) alle erforderlichen, grün markierten "OKs" zu holen. Führt eine (angekreuzte) Aussage zu einem einzelnen OK ("→ **hier alles OK**"), so bedeutet dies, dass die Anforderung grundsätzlich erfüllt ist. Führt eine Aussage zu einem mit einer Zahl versehenen OK (z.B. "→ **1. OK**"), so ist damit nur eines von mehreren erforderlichen OKs geholt (im Beispiel ist dann noch ein zweites OK, ev. ein drittes OK, usw. zu holen). Wie viele OKs erforderlich sind, damit eine Anforderung grundsätzlich erfüllt ist, ergibt sich aus dem Fragebogen. Führt eine Aussage zu einem roten "Bömbchen" ("💣") ist die Anforderung vermutlich nicht bzw. nicht vollständig erfüllt. Mit diesen beiden Codierungen kann derjenige, der das Formular ausfüllt, selbst beurteilen, ob seine Datenbearbeitung je nach der von ihm getroffenen Aussage die jeweilige Anforderung erfüllt.

   – Das Formular dokumentiert nur die Aussagen desjenigen, der das Formular ausfüllt. Es liefert für diese Aussagen keine Belege oder nähere Erläuterungen, auch wenn solche in den Freitext-Feldern vermerkt werden können (und sich gewisse Angaben aus dem Inventar, d.h. dem Formular B.2 und Formular B.3, ergeben). Die nötige Dokumentation und die nötigen Abklärungen, um das Formular ausfüllen zu können, sind Sache der Person, die es ausfüllt. Immerhin macht es Sinn, in einem der passenden Freitext-Felder festzuhalten, warum eine bestimmte Aussage getroffen wurde, wenn dies für einen Leser unklar wäre.

   – In der rechten Spalte kann nach dem Ausfüllen der mittleren Spalte angegeben werden, ob die betreffende Anforderung erfüllt ist oder nicht. Das ist ein Risikoentscheid; es ist möglich, die Anforderung als erfüllt zu erklären, auch wenn sie es in gewissen Konstellationen nicht

sein mag, diese Ausnahmen im Gesamtkontext aber von untergeordneter Bedeutung sind. In der rechten Spalte kann aber auch aus einer Reihe von vordefinierten Massnahmen zur Behebung etwaiger Nonkonformitäten oder anderer datenschutzrechtlicher Probleme, die sich aus der Beurteilung in der mittleren Spalte ergeben, ausgewählt werden. Findet sich keine passende Massnahme, kann sie auch frei formuliert werden. Es sind dies alles Vorschläge für Massnahmen, d.h. was genau umgesetzt wird und mit welcher Priorität ist damit noch nicht entschieden. Es liegt somit an der für eine Datenbearbeitung verantwortlichen Person, wie genau sie mit der Einhaltung des Datenschutzes nehmen will; sie wird dafür letztlich auch verantwortlich gemacht werden können.

– In Unternehmen mit komplexeren Verhältnissen greifen verschiedene Datenbearbeitungen regelmässig in sich. So landen z.B. die Daten aus der Bestellabwicklung im Data Warehouse oder die Firma, die für die technische Bereitstellung und den technischen Betrieb aller IT-Anwendungen zuständig ist, ist für die Speicherung aller Daten zuständig und müsste daher bei jeder Datenbearbeitung als Auftragsbearbeiter aufgeführt und behandelt werden. Das würde allerdings zu Doppelspurigkeiten führen. Aus diesem Grund ist es möglich, bestimmte Datenbearbeitungen ganz oder teilweise aus der Betrachtung beim Ausfüllen von Formular E.1 auszuklammern. Wird zum Beispiel die "Marktforschung" als eigene Datenbearbeitung beurteilt und greift diese auf die Daten vieler anderer Datenbearbeitungen im Unternehmen zu, so können die Verantwortlichen dieser Datenbearbeitungen die Marktforschung auf der Seite mit den "Abgrenzungen" ins erste Feld eingetragen werden. Sie brauchen sich dann bei der Beantwortung der Fragen nicht mehr um diese Zweitnutzung ihrer Daten zu kümmern (z.B. ob ihre Daten für die Marktforschung auch wirklich genutzt werden dürfen). Diese Fragen werden in diesem Falle nur noch bei der Beurteilung der Marktforschung geprüft. So verhält es sich im Prinzip auch bei den beiden weiteren Abgrenzungsmöglichkeiten. Im zweiten Feld könnte z.B. die "Stammdatenverwaltung" aufgeführt werden; greift dann der "Online-Shop" auf diese Datenbearbeitung zu, so braucht im Formular für den Online-Shop nicht geprüft werden, ob die Stammdatenverwaltung datenschutzkonform erfolgt. Es wird nur der Zugriff durch den Online-Shop geprüft.

– Im Formular E.1 wird an verschiedenen Stellen für bestimmte Fragestellungen auf Nebenformulare verwiesen. Diese sind dann beizuziehen und für die betreffende Datenbearbeitung parallel auszufüllen und das Ergebnis von dort in das Formular E.1 zu übernehmen. Will sich die verantwortliche Person für eine Datenbearbeitung zum Beispiel im Zusammenhang mit Anforderung nach Formular E.1 auf eine Einwilligung der betroffenen Person abstützen, so muss diese Einwilligung mit Q1 des Fragebogens von **Formular E.3** (DSGVO) bzw. **Formular E.4** (DSG) auf ihre Gültigkeit unter dem anwendbaren Datenschutzrecht geprüft werden (nebst anderen Rechtsgrundlagen bzw. Rechtfertigungsgründen). Diese Beurteilung kann im betreffenden Nebenformular dokumentiert werden. Wird dieselbe Einwilligung auch für eine andere Datenbearbeitung benötigt, kann auf dasselbe Nebenformular verwiesen werden. Für den Umgang mit Lösch- und Sperrrechten (unter der DSGVO) wird auf das **Formular E.5** verwiesen. Diese Nebenformulare haben keine eigenständige Bedeutung. Sie sind nur auszufüllen, wenn dies für die Beurteilung einer Datenbearbeitung gestützt auf Formular E.1 bzw. Formular E.2 nötig ist.

– Am Ende des Formulars E.1 können der oder die Eigner der von der Datenbearbeitung betroffenen Geschäftsprozesse für die Zwecke des

Risikomanagements eine Beurteilung abgeben, ob die Datenbearbeitung grundsätzlich datenschutzkonform ist, welche Risiken identifiziert und Massnahmen vorgeschlagen wurden und ob diese Risiken ins Risikoinventar des Unternehmens aufgenommen werden sollen. Dies beurteilt auch die Datenschutzstelle. Deren Beurteilung kann vom Prozesseigner wiederum kommentiert werden. Dieser Teil des Formulars ist optional.

Ist Formular E.1 oder Formular E.2 fertig ausgefüllt und sind die offenen Fragen geklärt, so können die Ergebnisse aus der rechten Spalte weiterverarbeitet werden. Wir empfehlen, diese in ein separates Dokument (z.B. eine Excel-Datei) zu übernehmen und dort weiterzuverarbeiten. Es muss entschieden werden, welche Massnahmen tatsächlich umgesetzt werden sollen und in welcher Priorität. Die diesbezüglichen Risikoentscheide bzw. deren Dokumentation sind derzeit nicht Teil von DSAT, ebenso nicht die Überwachung der Umsetzung der Massnahmen.

Ist die Datenschutz-Konformität einer Datenbearbeitung beurteilt, kann dies im Formular B.1 vermerkt werden.

6. In der Praxis hat es sich in mittleren und grösseren Unternehmen zudem als empfehlenswert erwiesen, ein **Verzeichnis** der Datenschutzerklärungen, Einwilligungserklärungen und -masken und weiteren offiziellen Dokumente mit Ausführungen zum Datenschutz zu führen, die mit dem Datenschutz zu tun haben. Dies hilft dem Unternehmen, den Überblick nicht zu verlieren, wo gegenüber betroffenen Personen welche Aussagen zum Datenschutz gemacht bzw. wo in welcher Form Einwilligungen abgeholt werden. Hierfür kann ebenfalls das **Formular B.1** benutzt werden. Diese Eintragungen sind jedoch optionaler Natur.

7. Soweit das Unternehmen eine Datenbearbeitung als Verantwortlicher bearbeitet, genügt die Beurteilung der Datenschutz-Konformität nach Formular E.1 unter Umständen nicht. Je nach Fallkonstellation wird zusätzlich zur herkömmlichen Konformitätsbeurteilung sowohl nach dem revidierten DSG als auch der DSGVO eine Datenschutz-Folgenabschätzung (**DSFA**) erforderlich sein. Hierfür wird das **Formular G.1** benutzt. In einem ersten Schritt wird damit beurteilt, ob eine DSFA überhaupt erforderlich ist. Dies geschieht durch das Ausfüllen des ersten Teils des Formulars. Ist eine DSFA nötig, kann diese mit demselben Formular durchgeführt werden. Auch dies ist Sache der für die Datenbearbeitung verantwortliche Person. Eine DSFA setzt ein fertig ausgefülltes Formular E.1 voraus. Ist die DSFA durchgeführt, kann dies im Formular B.1 vermerkt werden. Ist keine DSFA nötig, kann der Negativbefund zur Dokumentation ebenfalls abgelegt werden. Kleineren Unternehmen sei an dieser Stelle gesagt, dass sie diese Prozesse nicht unbedingt formalisieren müssen. Wesentlich ist, dass im Unternehmen jemand bestimmt ist, der sich in den jeweiligen Fällen der Sache annimmt und weiss oder herausfinden kann, was zu tun ist.

8. Im nächsten Schritt wird, soweit dies noch erforderlich ist, beurteilt, ob die vom Unternehmen in Anspruch genommenen Auftragsbearbeitungen den gesetzlichen Vorgaben entsprechen. Hierzu dient das **Formular F.1**, wobei für jede Auftragsbearbeitung (d.h. in der Regel jeden Auftragsbearbeiter und jeden Vertrag) ein separates Formular ausgefüllt werden muss (aus der Warte des Verantwortlichen; für Auftragsbearbeiter ist Formular E.2 vorgesehen). Auf Formular F.1 wird auch von Formular E.1 verwiesen. Da für die Auftragsbearbeitungen in den meisten Unternehmen andere Personen verantwortlich sind als jene, die für die Datenbearbeitungen verantwortlich zeichnen, und dieselbe Auftragsbearbeitung mehrere Da-

tenbearbeitungen betreffen kann, ist für die Erfassung und Beurteilung der Auftragsbearbeitungen ein separates Formular vorgesehen.

9. Im selben Sinne separat beurteilt werden die Massnahmen zur Datensicherheit. Hierzu dient **Formular F.2**. Dies erfolgt in einem separaten Formular, weil die Verantwortung für die Datensicherheit in den meisten Unternehmen einer anderen Stelle zugeteilt ist als den Inhalt der Datenbearbeitung. Sie ist häufig auch übergreifend geregelt und implementiert. So genügt es in aller Regel, für mehrere oder alle Datenbearbeitungen das Formular einmal auszufüllen (und in Formular E.1 jeweils darauf zu verweisen).

10. Schliesslich wird mit **Formular F.3** das Weisungswesen im Unternehmen beurteilt. Es wird ermittelt, ob die erforderlichen Weisungen und Schulungen gegenüber den Mitarbeitern des Unternehmens bestehen und die Einhaltung kontrolliert wird. Es wird dabei zwischen einer allgemeinen Datenschutzweisung und sachspezifischen Weisungen (z.B. zur Weisungen zur Bearbeitung von Personaldaten) unterschieden (wobei der Begriff der Weisung breit zu verstehen ist; dies kann auch eine persönliche Unterrichtung sein und muss nicht zwingend schriftlich erfolgen). Das Formular listet stichwortartig auch die typischen Themen dieser Weisungen (wobei diese letztlich unternehmensspezifisch sind). Um insbesondere im Hinblick auf kleine Unternehmen keinen "Overkill" zu betreiben, sind die sachspezifischen Weisungen und Angaben zur Überprüfung der Einhaltung der Weisung als "optional" angegeben, d.h. nicht jedes Unternehmen braucht dieses sachspezifischen Weisungen. Sie richten sich zudem eher an die Spezialisten, die auch wissen werden, wie entsprechende Weisungen zu formulieren sind und das Formular als Checkliste benutzen. Immerhin gibt die Auflistung auch dem kleineren Unternehmen Hinweise darauf, wo der Datenschutz im Unternehmen überall ein Thema sein kann.

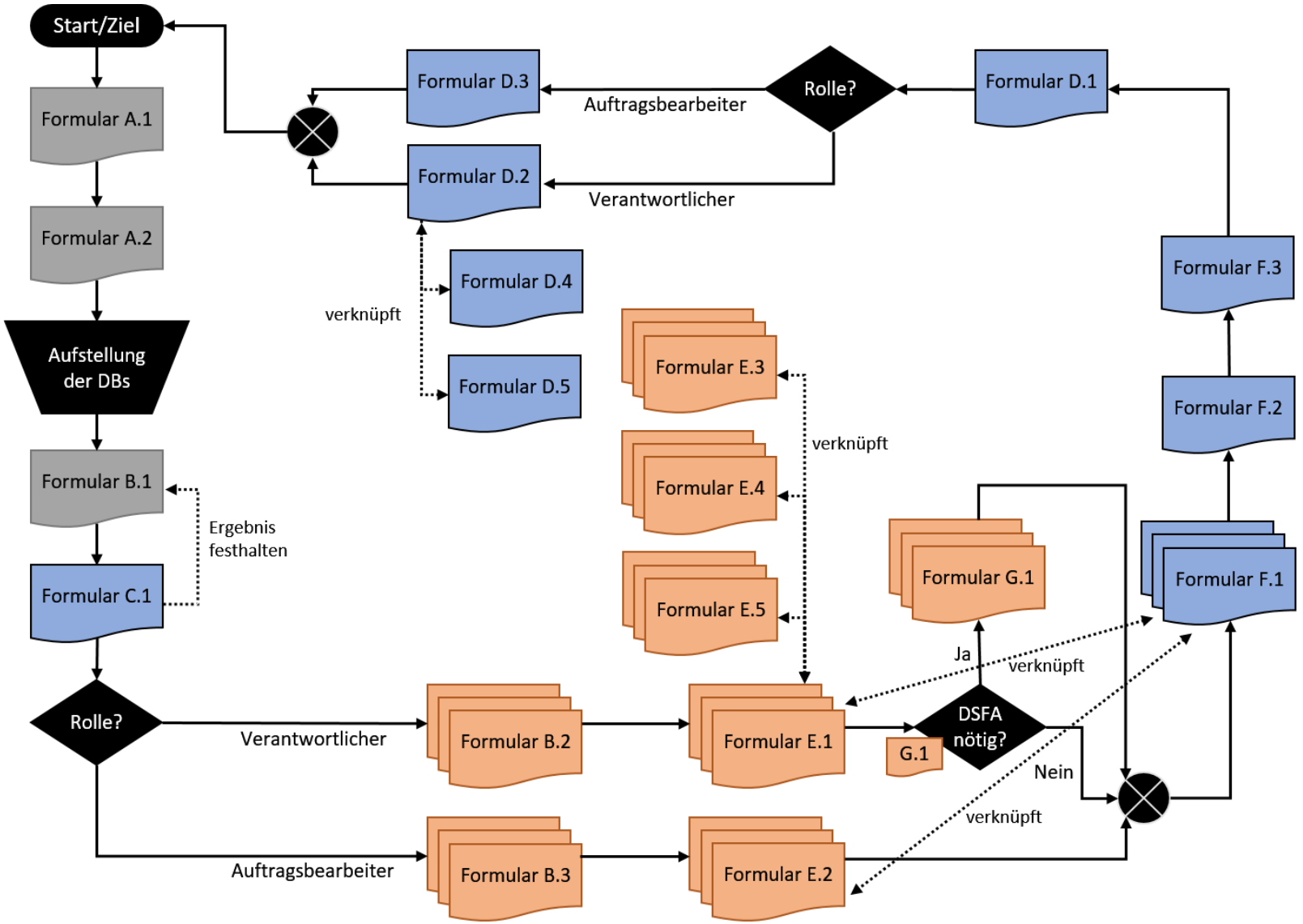
11. Soweit das Unternehmen mit einer oder mehreren Datenbearbeitungen in den Anwendungsbereich der DSGVO fällt, ist mittels **Formular D.1** in einem ersten Schritt zu prüfen, ob das Unternehmen einen Vertreter nach Art. 27 DSGVO, einen Datenschutzbeauftragten nach Art. 37 DSGVO oder beides bestellen muss. Hierbei werden nur die Vorgaben gemäss DSGVO geprüft, nicht etwaige strengere Vorgaben gemäss nationalem Recht der EU-Mitgliedstaaten. Diese sind insbesondere in den Fällen zu berücksichtigen, in denen sich die Unternehmenseinheit mit einer Niederlassung in der EU (bzw. dem EWR) befindet und mit einem lokalen Experten zu klären (bei Bedarf sollte mit diesem auch geklärt werden, inwieweit das nationale Recht auch extraterritorial, d.h. für Unternehmen in der Schweiz gilt). In Deutschland werden beispielsweise die meisten Unternehmen einen betrieblichen Datenschutzbeauftragten gemäss Art. 37 DSGVO ernennen müssen, weil das nationale Recht über die DSGVO hinausgeht. Ist ein Vertreter oder Datenschutzbeauftragter erforderlich, kann mit demselben Formular in einem zweiten Schritt geprüft werden, ob der Kandidat für eine solche Stelle bzw. die Vereinbarung mit diesem die gesetzlichen Anforderungen erfüllt. Die Dokumentation der Ernennung des Vertreters bzw. des Beauftragten erfolgt über Formular A.1.

12. In einem letzten Schritt ist zu beurteilen, ob das Unternehmen bzw. die einzelnen Unternehmensbereiche über die Prozesse verfügen, die gemäss dem revidierten DSG oder der DSGVO häufig erforderlich sind (z.B. der Prozess zur Meldung von Datensicherheitsverletzungen). Bestimmte dieser Prozesse (wie z.B. der Prozess zur Beantwortung des Auskunftsrechts) werden bereits im Rahmen der Beurteilung der einzelnen Datenbearbeitungen abgefragt, soweit sie sich darauf beziehen. Sie können jedoch dort ausgeklammert werden, wenn es effizienter erscheint, sie für mehrere Datenbearbeitungen zusammen zu beurteilen. Für die Beurteilung der Prozesse werden das **Formular D.2** und das **Formular D.3** be-

nutzt, je nachdem, ob das Unternehmen seine Rolle als Auftragsbearbeiter oder als Verantwortlicher beurteilt. Je nach Konstellation sind daher beide Formulare auszufüllen. Für das Formular D.2 werden sog. "Deep Dives" angeboten, Formulare für vertiefende Abklärungen, so namentlich für die Auskunftsprozesse (**Formular D.3**) und für den Prozess zur Meldung von Datensicherheitsverletzungen (**Formular D.4**).

Sind alle diese zwölf Schritte durchgeführt, ist die Beurteilung der Datenschutz-Konformität **komplett**. Wir empfehlen, die ausgefüllten Fragebogen an einem Ort zur Dokumentation des Datenschutzes im Unternehmen **aufzubewahren** und die Formulare nach Datum bzw. Versionsständen abzulegen, so dass immer klar ist, welches die neuste Fassung bzw. wie der Zustand früher war. Die Beurteilung der Datenschutz-Konformität ist kein einmaliger Vorgang, sondern ist immer dann selektiv zu **wiederholen**, wenn sich Änderungen im Betrieb ergeben, wenn neue Datenbearbeitungen hinzukommen oder sich Datenbearbeitungen ändern. Wir empfehlen ferner, dass die Verantwortlichen für eine Datenbearbeitung, die ihre Datenbearbeitung betreffenden Formulare und die darin enthaltenen Angaben bzw. Beurteilungen in periodischen Abständen auf ihre Richtigkeit und Vollständigkeit überprüfen. Bei Datenschutz-Folgenabschätzungen wird erwartet, dass diese mindestens alle drei Jahre wiederholt werden. Da sich die Formulare von DSAT ständig weiterentwickeln, ist darauf zu achten, dass jeweils die **neusten Fassungen** eingesetzt werden.

Inzwischen finden sich auf DSAT auch erste Vorlagen für **datenschutzrechtliche Dokumente**. Diese können grundsätzlich auch ohne Experten benutzt werden. Sie enthalten dazu jeweils entsprechende Anweisungen und Hinweise.


Start/Ziel
Formular A.1
Formular A.2
Aufstellung der DBs
Formular B.1
Formular C.1
Ergebnis festhalten
Rolle?
Verantwortlicher
Auftragsbearbeiter
Formular B.2
Formular B.3
Formular D.3
Formular D.2
Rolle?
Auftragsbearbeiter
Verantwortlicher
Formular D.1
verknüpft
Formular D.4
Formular D.5
Formular E.3
Formular E.4
Formular E.5
verknüpft
Formular E.1
Formular E.2
Formular G.1
Ja
verknüpft
DSFA nötig?
G.1
Nein
verknüpft
Formular F.3
Formular F.2
Formular F.1

Glossar

Begriff (alphabetisch)	Definition
Auftragsbearbeiter	Private Person, juristische Person, Personenvereinigung oder Bundesorgan, die oder das im Auftrag des Verantwortlichen (siehe Glossar) Personendaten bearbeitet. Unter der DSGVO ist vom "Auftragsverarbeiter" die Rede, was dasselbe meint.
BCR	"Binding Corporate Rules" oder "verbindliche Unternehmensregelungen", dienen als Basis für die Übermittlung personenbezogener Daten in Drittstaaten, auch innerhalb des gleichen Konzerns. Normalerweise ist das ein Vertrag zwischen den verschiedenen Unternehmenseinheiten, in welchem sich diese zur Einhaltung einheitlicher Datenschutzregeln verpflichten. Die Vereinbarung von BCR unterscheidet sich von der konzerninternen Vereinbarung der EU-Musterklauseln typischerweise dadurch, dass BCR konzernspezifisch angepasst werden können, während die Musterklauseln unverändert übernommen werden müssen. Die Regelungen sind aber oft ähnlich. BCR müssen vor dem Einsatz behördlich genehmigt werden.
Besondere Kategorien von Personendaten nach DSGVO	Als besondere Kategorien von personenbezogenen Daten gelten → personenbezogene Daten, aus denen die rassische und ethische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische (Personen-)Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Personendaten zum Sexualleben oder der sexuellen Orientierung ,. Die besonderen Kategorien von Personendaten nach DSGVO entsprechen ungefähr den "besonders schützenswerten Personendaten" im DSG. Vgl. auch → Strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmassregeln.
Besonders schützenswerte Personendaten (nach DSG)	Unterart der → Personendaten im DSG und Schweizer Variante der "besonderen Kategorien" von Personendaten unter der DSGVO. Es sind dies Personendaten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe (u.a. Sozialhilfe, Fürsorge, Kindes- und Erwachsenenschutzmassnahmen), administrative oder strafrechtliche Verfolgungen oder Sanktionen.
Gesetz im formellen Sinn (DSG)	Bundesgesetz oder für die Schweiz verbindliche Beschlüsse internationaler Organisationen und von der Bundesversammlung genehmigte völkerrechtliche Verträge mit rechtsetzendem Inhalt.
Medienprivileg (DSG)	Soweit Personendaten ausschliesslich zur Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet, kann der Verantwortliche unter dem DSG aus einem der folgenden Gründe die Auskunft verweigern, einschränken oder aufschieben: – Die Daten geben Aufschluss über die Informationsquellen – Durch die Auskunft würde Einsicht in Entwürfe für Publikationen gewährt

Begriff (alphabetisch)	Definition
	– Die Veröffentlichung würde die freie Meinungsbildung des Publikums gefährden Medienschaffende können die Auskunft zudem verweigern, einschränken oder aufschieben, wenn ihnen die Personendaten ausschliesslich als persönliche Arbeitsinstrumente dienen.
Personenbezogene Daten (DSGVO)	Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, wie Standortangaben, Namen, Informationen zu psychischen, physischen, kulturellen, wirtschaftlichen oder sozialen Eigenschaften einer natürlichen Person. Im DSG ist von "Personendaten" die Rede. Im vorliegenden Kontext wird der Begriff synonym gebraucht und es wird nur "Personendaten" verwendet, auch im Bereich der DSGVO. Für die vorliegenden Zwecke empfehlen wir, auch IP-Adressen und dauerhafte *Cookies* im Bereich der DSGVO als Personendaten zu betrachten, auch wenn sie es in vielen Fällen streng genommen nicht sind.
Personendaten (DSG)	Alle Angaben, die sich auf einer bestimmten oder bestimmbaren Person beziehen, d.h. jede Art von Information, unabhängig von der Herkunft, Form oder Darstellung. Beispiele sind Namen, als Namensersatz dienende Angaben, äusserliche körperliche Merkmale, innere geistige Zustände, Handlungen, Äusserungen, Verbindungen und Beziehungen usw. Die Person muss wenigstens bestimmbar sein. Sind die Daten anonymisiert, indem der Personenbezug irreversibel so aufgehoben wird, dass ohne unverhältnismässigen Aufwand keine Rückschlüsse auf Personen mehr möglich sind, ist die Person nicht (mehr) bestimmbar. Kann eine Person jedoch indirekt, mit Hilfe von weiteren, verfügbaren Datenquelle (z.B. Internet, eigene Datenbanken) identifiziert werden, ist die Person bestimmbar und es liegen mindestens aus Sicht der Person, die über diese weiteren Datenquellen verfügt, Personendaten vor.
Profiling (DSG)	Die Bewertung bestimmter Merkmale einer Person auf der Grundlage von automatisiert bearbeiteten Personendaten, insbesondere um die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, das Verhalten, die Vorlieben, den Aufenthaltsort oder die Mobilität zu analysieren oder vorherzusagen. Erfasst sind dabei laut der Botschaft des Bundesrats nur automatisierte Vorgänge, also nicht diejenige, die auch zum Teil einen relevanten "menschlichen" Entscheidungsvorgang mitenthalten. Entstehen durch die Bearbeitung anonyme Daten, ist das Profiling nicht datenschutzrelevant.
Profiling (DSGVO)	Jeder Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine Natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen. Es werden auch nur teilweise automatisierte Vorgänge erfasst. Entscheidend ist, ob aus dem Datenbild einer Person eine Schlussfolgerung mit Bezug auf persönliche Aspekte dieser Person gezogen wird. Entstehen durch die Bearbeitung anonyme Daten,

Begriff (alphabetisch)	Definition
	ist das Profiling nicht datenschutzrelevant.
Sichere Drittstaaten	Dies sind aus Sicht der EU bzw. der Schweiz jene Staaten, die über ein angemessenes, gesetzliches Datenschutzniveau verfügen und daher keine besonderen Vorkehrungen nötig sind, wenn Daten in diese Länder bekanntgegeben werden. Die Schweiz folgt im Wesentlichen der Beurteilung der EU, welche Drittstaaten als sicher gelten. Dies sind derzeit (März 2018) Andorra, Argentinien, Kanada (kommerzielle Unternehmen), Faroer, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Uruguay und – soweit das betreffende Empfänger-Unternehmen für die betreffenden Personendaten aus der EU bzw. der Schweiz "Privacy Shield"-zertifiziert ist – die USA. Auch die Schweiz gilt aus der Sicht der EU als sicheres Drittland. Den EU-Staaten gleichgestellt und somit ebenfalls sicher sind die Staaten des EWR (Liechtenstein, Norwegen, Island). Gespräche der Europäischen Kommission laufen derzeit mit Japan und Südkorea. Kein sicherer Drittstaat ist Australien (hier besteht nur ein Abkommen betr. Fluggastdaten). Aktuelle Liste: https://goo.gl/YvLDUp.
Strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmassregeln (DSGVO)	Personendaten über bereits abgeschlossene Strafverfahren und Urteile sowie über Straftaten, die (noch) nicht gerichtlich beurteilt wurden, in welchen jedoch einen konkreten begründeten Verdacht gegen eine bestimmte Person vorliegt, sowie Sicherungsmassregeln, die mit den Straftaten zusammenhängen, wie ein verhängtes Berufsverbot. Solche Daten dürfen nur sehr eingeschränkt verarbeitet werden.
Überwiegende Interessen Dritter (DSG)	Diese spielen insbesondere bei Auskunftsersuchen eine Rolle. Verlangt eine Person Auskunft über die von ihr bearbeiteten Daten, kann dies das Interesse auch anderer Personen tangieren, z.B. wenn diese darin ebenfalls vorkommen (weil beispielsweise ein Vorfall mehrere Personen betrifft oder Aussagen auch Auskunft über Dritten geben.). Überwiegen die Interessen der Dritten an der Nichtnennung die Interessen des Auskunftssuchenden überwiegen, kann die Auskunft eingeschränkt oder verweigert werden. Das Interesse der Dritten überwiegt dann, wenn das Interesse legitim ist und zumindest eine gewisse Erheblichkeit der Beeinträchtigung der Position des bzw. der Dritten vermutet werden kann. Nebst den Fällen des Auskunftsrechts können Interessen Dritter auch bei der Informationspflicht oder generell im Rahmen der Rechtfertigung von Persönlichkeitsverletzungen berücksichtigt werden. Im letzteren Falle zählen sie zu den "privaten" Interessen, die zusammen mit den Interessen des Datenbearbeiters, jene der betroffenen Person überwiegen können (vgl. → überwiegendes eigenes Interesse).
Überwiegendes eigenes Interesse (DSG)	Eine Datenbearbeitung, die persönlichkeitsverletzend ist, kann gerechtfertigt sein, wenn die eigenen Interessen der bearbeitenden Person an der Datenbearbeitung die Interessen der betroffenen Person, dass ihre Daten nicht bearbeitet werden, überwiegen. Ein überwiegendes eigenes Interesse des Datenbearbeiters kommt gemäss DSG insbesondere für die folgenden Fälle in Betracht: – Die Datenbearbeitung erfolgt im Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags mit der betroffenen Person.

Begriff (alphabetisch)	Definition

	– Der Datenbearbeiter steht der betroffenen Person in wirtschaftlichem Wettbewerb oder wird in wirtschaftlichen Wettbewerb treten und bearbeitet zu diesem Zweck Personendaten, die Dritten nicht bekanntgegeben werden.
	– Der Datenbearbeiter bearbeitet Personendaten zur Prüfung der Kreditwürdigkeit der betroffenen Person, wobei die folgenden Voraussetzungen erfüllt sind:
	  – Es handelt sich weder um besonders schützenswerte Personendaten noch um ein Profiling.
	  – Die Daten werden Dritten nur bekanntgegeben, wenn diese die Daten für den Abschluss oder die Abwicklung eines Vertrags mit der betroffenen Person benötigen.
	  – Die Daten sind nicht älter als fünf Jahre.
	  – Die betroffene Person ist volljährig.
	– Der Datenbearbeiter bearbeitet die Personendaten beruflich und ausschliesslich zur Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums.
	– Der Datenbearbeiter bearbeitet die Personendaten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung oder Statistik, wobei die folgenden Voraussetzungen erfüllt sind:
	  – Die Daten werden anonymisiert, sobald der Bearbeitungszweck es erlaubt.
	  – Besonders schützenswerte Personendaten werden Dritten so bekanntgegeben, dass die betroffenen Personen nicht bestimmbar sind.
	  – Die Ergebnisse werden so veröffentlicht, dass die betroffenen Personen nicht bestimmbar sind.
	– Der Datenbearbeiter sammelt Personendaten über eine Person des öffentlichen Lebens, die sich auf das Wirken dieser Person in der Öffentlichkeit beziehen.
	Die Aufzählung ist nicht abschliessend. Es sind weitere Fälle von überwiegenden eigenen Interessen denkbar. Eine detaillierte Beurteilung erfolgt im Rahmen von Formular E.4.
	Ebenso kann für die Verweigerung einer Auskunft über die Datenbearbeitung ein überwiegendes eigenes Interesse des Datenbearbeiters eine Rolle spielen. Die Interessen des privaten Inhabers der Datensammlung müssen die Interessen des Gesuchstellers überwiegen, was im Rahmen einer Abwägung der Interessen im Einzelfall beurteilt wird. Typische eigene Interessen im Zusammenhang mit dem Auskunftsrecht sind zum Beispiel der Schutz von Geschäftsgeheimnissen oder wo die Auskunft einen hohen finanziellen Aufwand mit sich bringen würde. Die Berufung auf ein überwiegendes eigenes Interesse im Rahmen des Auskunftsrechts ist nur gestattet, wenn die Daten nicht an Dritte bekanntgegeben werden.

Verantwortlicher	Private Person, juristische Person, Personenvereinigung oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet. Sie ist quasi der "Herr der Daten". Wenn ein Unternehmen eine Dienstleistung anbietet und hierfür die Adressdaten seiner Kunden bearbeitet, um diese mit der Dienst-

Begriff (alphabetisch)	Definition
	leistung versorgen zu können, tritt das Unternehmen als Verantwortlicher auf. Das tut es ebenfalls, wenn es die Personaldaten seiner Mitarbeiter bearbeitet. Betreibt ein Unternehmen hingegen die IT für ein anderes Unternehmen, ist es in aller Regel nicht ein Verantwortlicher, sondern das Gegenstück dazu, nämlich ein Auftragsbearbeiter.