Die Informationspflicht bei einer Verletzung der Datensicherheit – unter besonderer Beachtung von Bankdaten

Dissertationszusammenfassung

Célian Hirsch*

SCHLAGWÖRTER Datenschutz – Bankenrecht – Datensicherheit – Bankgeheimnis – Verletzung der Datensicherheit

I. Begriffe und Definitionen

Der erste Teil der Dissertation[1] befasst sich mit den Begriffen der Personendaten, der Bankdaten und der Verletzung der Datensicherheit.

A. Einleitung : Einführung und zentrale Begriffe des Datenschutzgesetzes

Sobald Personendaten bearbeitet werden, gilt das Datenschutzgesetz. Als solche Personendaten gelten alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Seit der Revision des DSG werden Angaben über juristische Personen zwar nicht mehr erfasst. Geschützt werden diese jedoch weiterhin durch ihr Recht auf informationelle Selbstbestimmung gegenüber dem Staat und durch den Persönlichkeitsschutz gegenüber Privatpersonen.[2] Um die Anwendbarkeit des DSG und somit die Informationspflicht einzuschränken, können die Daten auch pseudo- oder anonymisiert werden, sofern hierbei die Identifikation der natürlichen Person mit vernünftigem Aufwand und unter Berücksichtigung der konkreten Interessen des Dateninhabers verunmöglicht wird.[3]

B. Schutz von Bankdaten und Bankgeheimnis

Bankdaten werden sowohl durch das DSG als auch durch das Bankgeheimnis geschützt. Während das Bankgeheimnis nur zugunsten der Kunden gilt, unabhängig davon, ob es sich um natürliche oder juristische Personen handelt, gilt das DSG immer dann, wenn die Bank als Verantwortliche Daten von (natürlichen) Personen bearbeitet. Da das Bankgeheimnis nur Angaben eines bestimmten oder bestimmbaren Kunden schützt, kann dieser Schutz – wie im Datenschutzrecht – durch Pseudonymisierung und Anonymisierung begrenzt werden.[4] Von Bedeutung ist schliesslich noch der mit dem FINMA-Rundschreiben 2023/1 eingeführte Begriff der «kritischen Daten». Diese umfassen alle Daten, die im Hinblick auf die Grundsätze der Informationssicherheit, d.h. Vertraulichkeit, Verfügbarkeit und Integrität, geschützt werden müssen, und gehen somit über den Begriff der Personendaten hinaus.[5]

C. Verletzung der Datensicherheit und deren Auswirkungen

Die Verletzung der Datensicherheit wird definiert als eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Dieser weite Begriff wurde aus der DSGVO übernommen und entspricht ihr vollständig. Die ersten fünf Alternativen, die diese Definition aufführt, erfordern ein Ergebnis, welches im Verlust der Daten, deren unbeabsichtigter oder rechtswidriger Veränderung oder in deren unbefugter Offenlegung bestehen kann. Die letztgenannte Alternative erfordert hingegen nur eine konkrete Gefährdung,

* Célian Hirsch, Dr. iur., ist Rechtsanwalt und Oberassistent am Zentrum für Bank- und Finanzrecht der Universität Genf. Ein herzlicher Dank geht an Frau Milena Hendriks, LL.M. (Heidelberg) für die sorgfältige und wertvolle Überarbeitung dieses Artikels. Ihre Unterstützung hat massgeblich zur Qualität des Textes beigetragen.
 DOI dieses Artikels: 10.3256/978-3-03929-069-7_10.

1 Hirsch Célian, Le devoir d'informer lors d'une violation de la sécurité des données, Avec un regard particulier sur les données bancaires, thèse, Genève 2023.

2 Hirsch (Fn. 1), 18 ff.

3 Hirsch (Fn. 1), 33 ff.

4 Hirsch (Fn. 1), 60 ff.

5 Hirsch (Fn. 1), 62 ff.

die in der Möglichkeit besteht, dass eine unbefugte Person auf die Daten zugreifen könnte. Eine tatsächliche Kenntnisnahme ist nicht vorausgesetzt. Das Vorliegen einer solchen Zugriffsmöglichkeit wird anhand des vernünftigerweise getroffenen Aufwandes des Nichtberechtigten sowie seines konkreten Interesses beurteilt.[6] Die Verletzung der Datensicherheit ist vom Grundsatz der Datensicherheit zu unterscheiden. Letzterer verpflichtet jeden Verantwortlichen, dem Risiko angemessene technische und organisatorische Massnahmen zur Vermeidung von Verletzungen der Datensicherheit zu treffen. Das Vorliegen einer Verletzung der Datensicherheit lässt jedoch nicht zwangsläufig auf eine Verletzung des Grundsatzes der Datensicherheit schliessen, und umgekehrt.[7]

II. Funktionen und Rechtsquellen der Informationspflicht

Der zweite Teil der Arbeit untersucht die Funktionen sowie die Rechtsquellen und Voraussetzungen der Informationspflicht bei einer Verletzung der Datensicherheit.

A. Präventive und schützende Funktionen der Informationspflicht

Die Funktionen der Informationspflicht variieren je nach Empfänger. Ist die Information an die Behörde gerichtet, ermöglicht sie dieser, die Datensicherheit zu überwachen, die Einhaltung der Informationspflicht gegenüber den betroffenen Personen zu überprüfen und gegebenenfalls den Verantwortlichen, der Opfer der Verletzung der Datensicherheit wurde, zu unterstützen. Die Informationspflicht entfaltet auch eine präventive Wirkung, die zur Verbesserung der Datensicherheit beiträgt.[8] Ist die Information hingegen an die Person gerichtet, die durch die Verletzung der Datensicherheit betroffen ist, verfolgt sie mehrere Ziele, die im Folgenden nach ihrer Bedeutung absteigend aufgezählt werden: Schutz der Persönlichkeit und der Grundrechte der betroffenen Person; präventive Wirkung zugunsten der Datensicherheit; Vertrauen zwischen dem Verantwortlichen und der betroffenen Person; Möglichkeit der betroffenen Person, ihre Ansprüche durchzusetzen; und schliesslich die Gültigkeit der Einwilligung.[9] Die Sanktionierung stellt hingegen kein Ziel der Informationspflicht dar.[10] Begrenzt ist die Informationspflicht schliesslich durch die Überinformation, sowohl gegenüber der Behörde als auch der betroffenen Personen. Der Empfänger, der ständig über Verletzungen der Datensicherheit informiert wird, entwickelt eine *notification fatigue*, die dazu führen kann, dass er im Fall einer erheblichen Verletzung der Datensicherheit nicht mehr reagiert.[11]

B. Informationspflicht gegenüber Behörden und betroffenen Personen

Das Datenschutzgesetz von 1992 sah keine ausdrückliche Pflicht zur Information des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) bei einer Verletzung der Datensicherheit vor.[12] Erst 2018 wurde diese Verpflichtung durch die modernisierte Konvention 108 und die DSGVO eingeführt. So sieht Art. 33 DSGVO vor, dass die Aufsichtsbehörde über alle Verletzungen der Datensicherheit informiert werden muss, es sei denn, diese führt voraussichtlich zu keinem Risiko für die betroffenen Personen. Das Risiko umfasst einerseits die Schwere der möglichen Folgen der Verletzung der Datensicherheit und andererseits die Wahrscheinlichkeit, dass diese Folgen eintreten.[13] Der Schweizer Gesetzgeber hat diesen risikobasierten Ansatz übernommen, die Schwelle jedoch höher angesetzt. Gemäss Art. 24 Abs. 1 DSG ist der EDÖB nur dann über eine Verletzung der Datensicherheit zu informieren, wenn diese voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Wie unter der DSGVO muss der Verantwortliche eine Risikoanalyse vornehmen und dabei die Art, den Umfang und den Inhalt der betroffenen Daten, die Art und die Umstände der Verletzung der Datensicherheit, die Anzahl der betroffenen Personen sowie die Leichtigkeit ihrer Identifizierung berücksichtigen.[14] EU-Recht und schweizerisches Recht unterscheiden sich besonders hinsichtlich der Information der betroffenen Person. Art. 34 DSGVO verfolgt weiter einen risikobasierten Ansatz: Die betroffene Person muss informiert werden, wenn die Verletzung voraussichtlich zu einem hohen Risiko führt. Dagegen verpflichtet Art. 24 Abs. 4 DSG zur Information der betroffenen Person, wenn dies zu ihrem Schutz erforderlich ist, un-

6 Hirsch (Fn. 1), 71 ff.
7 Hirsch (Fn. 1), 77 ff.
8 Hirsch (Fn. 1), 100 ff.
9 Hirsch (Fn. 1), 110 ff.
10 Hirsch (Fn. 1), 117 f.
11 Hirsch (Fn. 1), 118 ff.
12 Hirsch (Fn. 1), 134 f.
13 Hirsch (Fn. 1), 137 ff.
14 Hirsch (Fn. 1), 144 ff.

abhängig vom Risiko.[15] Schliesslich trifft auch den Auftragsbearbeiter eine Informationspflicht zugunsten des Verantwortlichen, und zwar ebenfalls risikounabhängig.[16]

Zivilrechtlich kann eine Informationspflicht aus dem Grundsatz von Treu und Glauben abgeleitet werden. Diese unterscheidet sich von der im DSG vorgesehenen Informationspflicht, da sie sich nicht nur an die betroffenen natürlichen Personen richtet, sondern auch an juristische Personen oder Dritte, die Massnahmen zugunsten der betroffenen Personen ergreifen können.[17] Das Persönlichkeitsrecht stellt hingegen keine Quelle für die Informationspflicht dar, obwohl die Verletzung der Datensicherheit die Persönlichkeit der betroffenen Person beeinträchtigen kann.[18] Gleiches gilt für den Gefahrensatz.[19] Andererseits kann die Verpflichtung zur Schadensminderung unter bestimmten Umständen eine Informationspflicht begründen, da die Information den möglichen Schaden des Verantwortlichen reduzieren kann.[20] Auf vertraglicher Ebene ergibt sich eine Informationspflicht sowohl aus dem Auftrag als auch aus dem Arbeitsvertrag. Im Auftragsrecht besteht sie, wenn die Verletzung der Datensicherheit ein Risiko für den Auftraggeber darstellt oder wenn sie aus einer Verletzung der Geheimhaltungspflicht des Beauftragten resultiert.[21] Im Arbeitsvertrag schulden beide Parteien ihrem Vertragspartner hinreichende Information. Der Arbeitgeber informiert den Arbeitnehmer, wenn die Verletzung der Datensicherheit ein Risiko für diesen darstellt. Umgekehrt hat der Arbeitnehmer den Arbeitgeber über jede Verletzung der Datensicherheit zu unterrichten, unabhängig vom Risiko.[22]

Im Finanzmarktrecht verpflichtet Art. 29 Abs. 2 FINMAG jeden Beaufsichtigten, der FINMA die Vorkommnisse zu melden, die für die Aufsicht von wesentlicher Bedeutung sind. Dies kann Verletzungen der Datensicherheit einschliessen. Handelt es sich beim Beaufsichtigten um eine juristische Person, so unterliegt sie selbst dieser Meldepflicht, und nicht ihre Organe.[23] Die Beauftragten von Banken, Versicherungen und Finanzinstituten unterliegen ebenfalls dieser Pflicht, ebenso wie die Prüfgesellschaften. Letztere haben die FINMA selbstverständlich nicht über selbst erlittene Verletzungen der Datensicherheit zu informieren, sondern über solche des Beaufsichtigten.[24] Die FINMA hat ihre Anforderungen hinsichtlich Cyberangriffen präzisiert. Ausserdem verlangt sie, über wichtige Vorfälle informiert zu werden, die kritische Daten betreffen. Eine eigentliche Pflicht, Kunden oder allgemein betroffene Personen im Falle einer Verletzung der Datensicherheit zu informieren, sieht das Finanzmarktrecht zwar nicht vor. Die FINMA verlangt allerdings von den Beaufsichtigten, dass sie auch ihre gesetzlichen Verpflichtungen aus anderen Rechtsgebieten als dem Finanzmarktrecht einhalten, einschliesslich des Datenschutzes. Durch die Anforderung, eine einwandfreie Geschäftsführung zu gewährleisten, kann die Behörde somit auch die Einhaltung der Informationspflicht gegenüber den betroffenen Personen durchsetzen.[25]

III. Umfang, Einschränkungen und Modalitäten der Informationspflicht

Im dritten Teil der Arbeit werden der Umfang, die Einschränkungen und die Modalitäten der Informationspflicht bei einer Verletzung der Datensicherheit erörtert.

A. Umfang der Informationspflicht je nach Empfänger

Der Umfang der geschuldeten Information variiert je nach Empfänger. Der Verantwortliche muss der Behörde (Aufsichtsbehörde eines EU-Mitgliedstaates, EDÖB oder FINMA) genauere Informationen mitteilen als der betroffenen Person. Die Behörde muss insbesondere über die Details der Verletzung der Datensicherheit sowie deren wahrscheinliche Folgen informiert werden, um zu überprüfen, ob die vom Verantwortlichen getroffenen oder geplanten Massnahmen seinen gesetzlichen Verpflichtungen genügen.[26] Die betroffene Person benötigt hingegen vereinfachte Informationen über die Verletzung sowie allgemeine Ratschläge zu den zu ergreifenden Massnahmen (beispielsweise Änderung eines Passworts). Die Erteilung individueller Ratschläge rechtfertigt sich insbesondere bei bestehendem Vertragsverhältnis zwischen Verantwortlichem und betroffener Person, wie im Auftrag oder Arbeitsvertrag.[27]

15 Hirsch (Fn. 1), 160 ff.
16 Hirsch (Fn. 1), 167 ff.
17 Hirsch (Fn. 1), 175 ff.
18 Hirsch (Fn. 1), 183 ff.
19 Hirsch (Fn. 1), 189 ff.
20 Hirsch (Fn. 1), 187 ff.
21 Hirsch (Fn. 1), 191 ff.
22 Hirsch (Fn. 1), 196 ff.
23 Hirsch (Fn. 1), 207 ff.
24 Hirsch (Fn. 1), 212 ff.
25 Hirsch (Fn. 1), 224 ff.
26 Hirsch (Fn. 1), 240 ff.
27 Hirsch (Fn. 1), 250 ff.

B. Einschränkungen der Informationspflicht durch das Prinzip *nemo tenetur* und Geheimhaltungspflichten

Eine Einschränkung der Informationspflicht gegenüber der Behörde sehen weder die DSGVO noch das schweizerische Recht vor. Dennoch kann der *Nemo tenetur*-Grundsatz eine solche Einschränkung darstellen, da niemand verpflichtet ist, sich selbst zu belasten.[28] Die Meldung einer Verletzung der Datensicherheit kommt jedoch potenziell einem Geständnis eines Verstosses gegen den Grundsatz der Datensicherheit gleich. Hinsichtlich der strengen Sanktionen der DSGVO ist die Informationspflicht insofern problematisch. Das deutsche Recht sieht daher ausdrücklich vor, dass der Bericht über die Verletzung der Datensicherheit nicht ohne Zustimmung des Verantwortlichen gegen diesen verwendet werden darf. In der Schweiz hingegen steht der *Nemo tenetur*-Grundsatz der Informationspflicht nicht entgegen. Tatsächlich bestraft das DSG die Verletzung dieser Informationspflicht nicht, und auch die Massnahmen der FINMA stellen laut Bundesgericht keine strafrechtlichen Sanktionen dar.[29] Bezüglich der Information der betroffenen Person sehen sowohl die DSGVO als auch das DSG ausdrücklich deren Einschränkung vor. So kann eine Geheimhaltungspflicht wie etwa das Bank- oder Anwaltsgeheimnis die Informationspflicht gegenüber der betroffenen Person einschränken, wenn diese nicht selbst Geheimnisherrin ist.[30] Die Einschränkung kann ausserdem auch das Kommunikationsmittel betreffen, sodass, wenn eine direkte Information unmöglich oder unverhältnismässig ist, der Verantwortliche eine öffentliche Mitteilung vornehmen muss.

C. Anforderungen an Form, Frist und Dokumentation der Information

Die Informationspflicht muss bestimmte Modalitäten einhalten. Das Gesetz stellt Anforderungen an Form und Frist und verlangt die Dokumentation der Verletzung. In der Praxis legt jede Behörde eigene Formvorschriften für die Meldung fest. Während die Information der betroffenen Person vor allem klar und verständlich sein soll, müssen Behörden besonders rasch informiert werden: Die DSGVO setzt eine feste Frist von 72 Stunden, das DSG und das FINMAG sind offener formuliert («so rasch als möglich» bzw. «unverzüglich»). Hinsichtlich der Informationsfrist der betroffenen Person weist das DSG eine Lücke auf, die dahingehend zu schliessen ist, dass auch diese Information «so rasch als möglich» zu erfolgen hat.[31] Die zentrale Frage betrifft jedoch weniger die Dauer der Frist, sondern ihr Beginn.[32] Der Moment der Kenntnis des Verantwortlichen von der Verletzung der Datensicherheit ist häufig nicht einfach zu bestimmen. Darüber hinaus muss dieser eine gestaffelte Meldung an die Behörde vornehmen, wenn er innerhalb der vorgegebenen Frist nicht über alle relevanten Informationen verfügt. Schliesslich verpflichtet die DSGVO den Verantwortlichen dazu, alle Verletzungen der Datensicherheit zu dokumentieren. Diese Verpflichtung wurde auch im Schweizer Recht übernommen – jedoch erst auf Verordnungsstufe, sodass diese mangels gesetzlicher Grundlage ungültig ist.[33]

IV. Übermittlung des Berichts an Strafverfolgungsbehörden

Der vierte Teil der Arbeit befasst sich mit der Übermittlung des Berichts über die Verletzung der Datensicherheit an die Strafverfolgungsbehörden sowie dem Auskunftsrecht hinsichtlich dieses Berichts.

A. Voraussetzungen für die Übermittlung an Strafverfolgungsbehörden

Deckt der Bericht über die Verletzung der Datensicherheit eine Verletzung des FINMAG oder der Finanzmarktgesetze auf, etwa eine Verletzung des Bank- oder Berufsgeheimnisses, ist die FINMA zur Information der zuständigen Strafverfolgungsbehörde verpflichtet. Geht aus dem Bericht demgegenüber eine Verletzung des DSG hervor, beispielsweise des Grundsatzes der Datensicherheit, kann die FINMA die Strafverfolgungsbehörde informieren; sie muss dies aber nicht. Auch der EDÖB hat zwar das Recht, nicht aber die Pflicht, die Strafverfolgungsbehörde über eine durch den Bericht entdeckte Verletzung des DSG zu informieren. Wird der Bericht an die Strafverfolgungsbehörde übermittelt, ist er nicht zwangsläufig verwertbar. Seiner Verwertbarkeit steht mitunter der *Nemo tenetur*-Grundsatz entgegen, wenn der Berichtspflichtige den Bericht unter der (auch abstrakten) Androhung einer Strafsanktion an die FINMA übermittelt hat. Dies gilt sowohl gegenüber dem Berichtspflichti-

[28] Hirsch (Fn. 1), 260 ff.
[29] Hirsch (Fn. 1), 282 ff.
[30] Hirsch (Fn. 1), 311 ff.
[31] Hirsch (Fn. 1), 355 ff.
[32] Hirsch (Fn. 1), 334 ff.
[33] Hirsch (Fn. 1), 331 ff.

gen als auch gegenüber den natürlichen Personen, die an der Erstellung des Berichts beteiligt waren.[34] Berichte, die durch den EDÖB übermittelt wurden, sind von Gesetzes wegen grundsätzlich unverwertbar. Eine Ausnahme besteht im Falle des Einverständnisses des Berichtspflichtigen.[35]

B. Auskunftsrechte und Einschränkungen des Zugangs zu Berichten

Auch wenn der Bericht über die Verletzung der Datensicherheit von einem Anwalt vorbereitet oder verfasst wurde, ist er nicht durch das Anwaltsgeheimnis geschützt.[36] Der Bericht unterliegt grundsätzlich der Rechenschaftspflicht (Art. 400 OR), da er kein rein internes Dokument darstellt.[37] Allerdings enthält der Bericht teilweise auch Elemente, die grundsätzlich durch das Geschäftsgeheimnis geschützt sind, sodass der Zugang dennoch eingeschränkt sein kann.[38] Er unterliegt jedoch nicht dem Auskunftsrecht nach Art. 25 DSG.[39] Für den Bericht gelten die gleichen Einschränkungen wie für die Rechenschaftspflicht im Rahmen des Herausgaberechts von Dokumenten nach Art. 72 FIDLEG.[40] Immerhin könnte das Öffentlichkeitsprinzip die Einsicht in den Bericht erlauben, wenn dieser an die FINMA oder den EDÖB übermittelt wurde. Die FINMA ist zwar im Prinzip vom Anwendungsbereich des Öffentlichkeitsgesetzes ausgenommen, gemäss Art. 10 EMRK kann jedoch unter bestimmten Voraussetzungen die Übergabe von Berichten über die Verletzung der Datensicherheit auch von ihr verlangt werden.[41] Der EDÖB untersteht seinerseits dem Öffentlichkeitsgesetz, sodass hier leichter die Einsicht in die Berichte verlangt werden kann. Dies wird jedoch durch das Geschäftsgeheimnis und den Schutz der Privatsphäre des Verantwortlichen eingeschränkt.[42] Schliesslich kann die Einsicht in den Bericht auch im Rahmen einer vorsorglichen Beweisführung verlangt werden oder gestützt auf die Mitwirkungspflicht im Rahmen des Hauptverfahrens. Allerdings kennt auch dieser Zugang bestimmte Einschränkungen, um die Interessen des Verantwortlichen zu schützen.[43]

V. Folgen einer Verletzung der Informationspflicht

Im letzten Teil der Arbeit werden die Folgen einer Verletzung der Informationspflicht bei einer Verletzung der Datensicherheit untersucht.

A. Zivilrechtliche Folgen einer Verletzung der Informationspflicht

Ein Verstoss gegen die Informationspflicht kann sowohl eine Vertragsverletzung als auch eine unerlaubte Handlung darstellen. Einen Schaden verursacht er, wenn die betroffene Person bei gehöriger Information bestimmte Massnahmen hätte ergreifen können, um eine Vermögensverminderung zu vermeiden, wie beispielsweise die Sperrung ihrer Kreditkarte, deren Daten gestohlen wurden.[44] Obwohl dieser Verstoss auch eine Persönlichkeitsverletzung darstellt, erreicht diese in der Regel nicht den ausreichenden Grad an Härte, um Genugtuung zu verlangen.[45] Jedoch sieht Art. 82 DSGVO ausdrücklich eine Entschädigung für «immateriellen Schaden» vor, deren Bedeutung der EuGH erst kürzlich näher erläutert hat. Die Prüfung des Verschuldens des Verantwortlichen hängt von der geltend gemachten Verletzung ab, je nachdem, ob ein Tätigwerden oder ein Erfolg geschuldet war. Die Verjährung für vertragliche Schadensersatzansprüche gegen den Verantwortlichen läuft ab dem Tag der Verletzung. Das Gleiche gilt für die absolute Frist im Falle eines ausservertraglichen Anspruchs. Der *dies a quo* der relativen Frist hängt von den konkreten Umständen des Einzelfalls ab.[46] Darüber hinaus kann ein Verstoss gegen die Informationspflicht im Arbeitsvertrag eine fristlose Vertragsauflösung rechtfertigen, sei es durch den Arbeitgeber oder den Arbeitnehmer; im Auftragsrecht kann er einen wichtigen Grund darstellen, der eine sofortige Beendigung des Vertrags ohne Entschädigungspflicht für den Kündigenden ermöglicht.[47] Schliesslich bewirkt die unterlassene Information die anfängliche Unmöglich-

34 Hirsch (Fn. 1), 374 ff.
35 Hirsch (Fn. 1), 384 ff.
36 Hirsch (Fn. 1), 392 ff.; vgl. Hirsch Célian, Le devoir d'informer de l'avocat lors d'une violation de la sécurité des données, Revue de l'avocat, 8/2024.
37 Hirsch (Fn. 1), 396 ff.
38 Hirsch (Fn. 1), 400 ff.
39 Hirsch (Fn. 1), 413 ff.
40 Hirsch (Fn. 1), 417 ff.
41 Hirsch (Fn. 1), 420 ff.
42 Hirsch (Fn. 1), 427 ff.
43 Hirsch (Fn. 1), 442 ff.
44 Hirsch (Fn. 1), 458 ff.
45 Hirsch (Fn. 1), 463 ff.
46 Hirsch (Fn. 1), 483 ff.
47 Hirsch (Fn. 1), 491 ff.

keit jeder Einwilligung zur Rechtfertigung einer Datenbearbeitung.[48]

B. Massnahmen der EDÖB und FINMA bei Verdacht auf Verletzung der Informationspflicht

Bei Verdacht eines Verstosses gegen die Informationspflicht können der EDÖB und die FINMA eine Vorabklärung durchführen. Kann der Verdacht nicht ausgeräumt werden oder erfüllt der Verantwortliche trotz Aufforderung der Behörde seine Pflicht nicht, kann diese ein formelles Verfahren gegen ihn einleiten. Nach Abschluss der Untersuchung kann der EDÖB hauptsächlich den Verantwortlichen anweisen, die Informationspflicht sowohl gegenüber der Behörde als auch gegenüber den betroffenen Personen einzuhalten.[49] Bei einem schwerwiegenden Verstoss ermöglicht das *Enforcement*-Verfahren der FINMA zudem den Erlass einer Feststellungsverfügung oder gar deren Veröffentlichung. Die anderen Massnahmen, die diesen beiden Behörden zur Verfügung stehen, sind hingegen bei einem Verstoss gegen die Informationspflicht in der Regel nicht angemessen.[50] Die FINMA und der EDÖB müssen zudem möglicherweise ihre Verfahren koordinieren.[51] Unterliegt ein in der Schweiz ansässiger Verantwortlicher oder Auftragsbearbeiter der DSGVO, kann ein Verstoss gegen die Informationspflicht ebenfalls von einer Aufsichtsbehörde eines EU-Mitgliedstaates sanktioniert werden. Im Gegensatz zum schweizerischen Recht kann diese Aufsichtsbehörde auch eine Verwaltungsstrafe auferlegen. Ihre Zustellung in der Schweiz ist jedoch aufgrund der Schweizer Souveränität und mangels einschlägiger internationaler Verträge mit Schwierigkeiten verbunden.[52]

C. Strafrechtliche Folgen einer Verletzung der Informationspflicht

Der Verstoss gegen die Informationspflicht ist weder gemäss StGB noch gemäss DSG strafbar, es sei denn, der EDÖB hat zuvor eine Verfügung mit Sanktionsandrohung getroffen.[53] Auch im FINMAG wird der Verstoss gegen die Informationspflicht nicht bestraft, es sei denn, der Berichtspflichtige teilt der Behörde eine unvollständige Information mit und erweckt dadurch einen falschen Eindruck. Von den Finanzmarktgesetzen sehen nur Art. 49 Abs. 1 lit. b BankG und Art. 149 Abs. 1 lit. d KAG eine strafrechtliche Sanktion bei Verletzung der Informationspflicht vor, wobei nach Art. 49 Abs. 2 BankG sogar Fahrlässigkeit strafbar ist.[54]

48 Hirsch (Fn. 1), 497.
49 Hirsch (Fn. 1), 500 ff.
50 Hirsch (Fn. 1), 507 ff.
51 Hirsch (Fn. 1), 510 ff.
52 Hirsch (Fn. 1), 522 ff.
53 Hirsch (Fn. 1), 528 ff.
54 Hirsch (Fn. 1), 534 ff.