



Eidgenössischer Datenschutzbeauftragter
Préposé fédéral à la protection des données
Incaricato federale per la protezione dei dati
Incumbensà federal per la protecziun da datas

Kundenbindungsprogramm M-CUMULUS

Schlussbericht

vom 23. Mai 2005

sowie

Anhang

vom 28. September 2005

**der Kontrolle des
Eidgenössischen Datenschutzbeauftragten (EDSB)
gemäss Art. 29 des Bundesgesetzes
über den Datenschutz (DSG)**

Veröffentlicht am 7. November 2005 auf www.edsb.ch

Inhaltsverzeichnis

Inhaltsverzeichnis.....	2
1. Ausgangslage	4
2. Umfang der Kontrolle	4
3. Chronologie der Kontrolle.....	4
4. Grundlagen des Kontrollberichtes.....	5
4.1 Eingereichte Dokumentation / beantwortete Fragen im Vorfeld der Kontrolle....	5
4.2 Kontrolle vom 2. Februar 2005 vor Ort in Zürich	6
4.2.1 Anwesende Personen	6
4.2.2 Besichtigte Anlagen/Präsentationen	6
4.3 Fact Sheet und beantwortete offene Fragen im Nachgang der Kontrolle	6
4.4 Schema der Datenflüsse im Rahmen von M-CUMULUS	6
5. Datenschutzrechtliche Beurteilung.....	7
5.1 Anmeldung.....	8
5.1.1 Untersuchte Datenflüsse.....	8
5.1.2 Anmeldung im Einzelnen	8
5.1.3 Beurteilung aus Sicht des EDSB	9
5.2 Punktesammlung.....	10
5.2.1 Untersuchte Datenflüsse.....	10
5.2.2 Punktesammeln im Einzelnen.....	10
5.2.3 Beurteilung aus Sicht des EDSB	11
5.3 Marketing	12
5.3.1 Untersuchte Datenflüsse.....	12
5.3.2 Marketing im Einzelnen.....	12
5.3.3 Beurteilung aus Sicht des EDSB	13
5.4 Werbung (von Migros)	14
5.4.1 Untersuchte Datenflüsse.....	14
5.4.2 Werbung im Einzelnen	14
5.4.3 Einige Zahlen zum Versand von Direktwerbung	16
5.4.4 Beurteilung aus Sicht des EDSB	16
5.5 Werbung (von Partnern)	17
5.5.1 Untersuchte Datenflüsse.....	17
5.5.2 Werbung von Partnern im Einzelnen	17
5.5.3 Beurteilung aus Sicht des EDSB	17
5.6 Auskunftsrecht.....	19
5.6.1 Untersuchter Datenfluss	19
5.6.2 Auskunftsrecht im Einzelnen	19
5.6.3 Beurteilung aus Sicht des EDSB	20
5.7 Datenauskünfte bei einer Straftat	22
5.7.1 Untersuchter Datenfluss	22
5.7.2 Weiterleitung von Kundendaten bei Straftaten im Einzelnen	22
5.7.3 Beurteilung aus Sicht des EDSB	23
5.8 Datenlöschung auf Verlangen der Kunden.....	24
5.8.1 Untersuchter Datenfluss	24
5.8.2 Löschanträge im Einzelnen	24
5.8.3 Beurteilung aus Sicht des EDSB	25

5.9 Aufbewahrung und Löschung weiterer Daten	26
5.9.1 Untersuchter Datenfluss	26
5.9.2 Aufbewahrung und Löschung weiterer Daten im Einzelnen	26
5.9.3 Beurteilung aus Sicht des EDSB	27
5.10 Sicherheit	28
5.10.1 Untersuchte Räume	28
5.10.2 Sicherheitsmassnahmen im Einzelnen	28
5.10.3 Beurteilung aus Sicht des EDSB	28
5.11 Sensibilisierung und Schulung von CUMULUS-Mitarbeitern	29
5.11.1 Ergriffene Massnahmen	29
5.11.2 Beurteilung aus Sicht des EDSB	29
6. Ergebnisse	30
6.1 Anmeldung	30
6.2 Punktesammlung	30
6.3 Marketing	30
6.4 Werbung (von Migros)	31
6.5 Werbung (von Partnern)	32
6.6 Auskunftsrecht	32
6.7 Datenauskünfte bei Straftaten	33
6.8 Datenlöschung auf Verlangen der Kunden	33
6.9 Aufbewahrung und Löschung weiterer Daten	33
6.10 Sicherheit	34
6.11 Sensibilisierung und Schulung von CUMULUS-Mitarbeitern	34
6.12 Datentransfer ins Ausland	34
7. Schlussfolgerungen	35
7.1 Bezüglich der Kontrolle des Kundenbindungsprogramms M-CUMULUS	35
7.2 Verfahren und weiteres Vorgehen	35
Anhang vom 28. September 2005 zum Schlussbericht	I
1. Vorbemerkung	I
2. Auswertung der Stellungnahme von Migros	I
2.1 Marketing	I
2.2 Werbung (von Migros)	II
2.3 Werbung (von Partnern)	II
2.4 Auskunftsrecht	III
2.5 Datenlöschung auf Verlangen der Kunden	III
2.6 Aufbewahrung und Löschung weiterer Daten	IV
2.7 Sicherheit	V
2.8 Datentransfer ins Ausland	V

1. Ausgangslage

Migros bietet ihren Kunden seit dem 1. November 1997 ein Bonusprogramm an, M-CUMULUS genannt. Bei jedem Einkauf können bei Vorweisen der CUMULUS-Karte Punkte gesammelt werden (je 1 Punkt pro 1.- CHF Umsatz). Der Punktestand wird alle zwei Monate zusammengezählt, und pro 500 Punkte erhalten die Kunden per Post einen CUMULUS-Bon im Wert von 5.- CHF. Ab einer gewissen Umsatzgrösse gibt es zusätzliche Treuepunkte. Daneben lanciert Migros regelmässig Bonus-Punkte Aktionen, bei denen mehrfache oder zusätzliche Punkte gesammelt werden können. Unabhängig vom Punktestand werden auch regelmässig Rabatt-Coupons verschickt. Die Migros-Kunden können ihre Bons innerhalb der Migros und diversen Migros-Unternehmen wie Bargeld einsetzen.

Kunden, die am Bonusprogramm teilnehmen, erlauben der Migros, detaillierte Informationen über ihre Einkäufe zu sammeln und für Marketingzwecke auszuwerten. M-CUMULUS-Teilnehmer erhalten gestützt auf ihre Einkaufsdaten konkrete Angebote und Informationen aus dem Migros-Sortiment, sofern sie nicht ausdrücklich darauf verzichten.

In der M-CUMULUS-Datenbank sind ca. 2 Mio. Haushalte erfasst und 2,3 Mio. Konten eingerichtet. Bei etwa 70% des Migros Detailhandelsumsatzes wird eine CUMULUS-Karte vorgezeigt und gepunktet. Ca. 95% aller CUMULUS-Bons werden von den Kunden auch tatsächlich wieder eingelöst.

Zur Durchführung des Kundenbindungsprogramms M-CUMULUS werden von der Migros, den Programm-Trägern¹ und den Programm-Partnern² Daten von Personen, die an diesem Programm teilnehmen, bearbeitet. Seit Lancierung des Kartenprogramms ist der Benutzerkreis stetig gewachsen. Eine Datenschutzkontrolle gemäss Art. 29 des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1) ist daher nicht zuletzt gestützt auf den grossen Benutzerkreis sowie gestützt auf die Sensibilität der bearbeiteten Personendaten von Bedeutung.

2. Umfang der Kontrolle

Die Datenschutzkontrolle des EDSB bezog sich auf die Datenabläufe im Rahmen des Kundenbindungsprogramms M-CUMULUS. Die Kontrolle fokussierte sich auf die internen Datenabläufe zwischen M-CUMULUS und den Migros-Unternehmen (Programm-Trägern) sowie auf die Datenflüsse zwischen der Migros und den Programm-Partnern. Die Programm-Partner selbst wurden weder einer näheren Überprüfung unterzogen, noch wurde speziell auf den Datenaustausch mit ausgewählten Programmpartnern eingegangen.

3. Chronologie der Kontrolle

3. Oktober 2004 Beschluss des EDSB zur Durchführung einer Datenschutzkontrolle beim Migros-Genossenschafts-Bund (im Folgenden MGB) im Rahmen des Kundenbindungsprogramms M-CUMULUS.

¹ Als *Programm-Träger* gelten die zur Migros-Gemeinschaft zählenden Firmen/Fachmärkte, bei denen gepunktet werden kann (z.B. Micasa, DO IT + GARDEN, sportXX, OBI, Migrol, Migrosbank)

² Als *Programm-Partner* gelten die NICHT zur Migros gehörenden Firmen, bei denen gepunktet werden kann (z.B. Mobility, Switzerland Travel Center, Le Shop.ch)

7. Dezember 2004	Ankündigung der Kontrolle beim MGB mit der Bitte um Dokumentation über das Kundenbindungsprogramm und Beantwortung von Zusatzfragen.
4. Januar 2005	Eingang der Unterlagen und Dokumente von Migros (eingereicht durch M-CUMULUS Marketing Services und MGB Rechtsabteilung).
2. Februar 2005	Durchführung der Datenschutzkontrolle vor Ort am Hauptsitz des MGB in Zürich.
4. Februar 2005	Der EDSB gibt per Email seine Vorstellungen für das weitere Vorgehen der Kontrolle an die Rechtsabteilung des MGB bekannt.
21. März 2005	Telefonische Rückfrage der Datenschutzbeauftragten des MGB an den EDSB bezüglich eines geplanten Datentransfers ins Ausland.
24. März 2005	Zusendung eines Fact Sheets der Datenschutzkontrolle vom 2. Februar 2005 an M-CUMULUS Marketing Services und die Rechtsabteilung MGB zur Konsultation. Zugleich Bitte des EDSB um materielle Berichtigung des Fact Sheets sowie Beantwortung noch offener Fragen.
1. April 2005	Telefonische Rückmeldung des Leiters M-CUMULUS Marketing Services auf das Fact Sheet und mündliche Übermittlung der Korrekturen.
5. April 2005	Eingang der Antworten auf die noch offenen Fragen des EDSB (durch M-CUMULUS Marketing Services) sowie Eingang der Anmeldung einer Datenübermittlung ins Ausland gemäss Art. 6 DSGVO.
13. April 2005	Der EDSB schickt ein Schema der Datenflüsse im Rahmen von M-CUMULUS an M-CUMULUS Marketing Services mit der Bitte, das Schema zu ergänzen oder zu korrigieren. Das Schema wurde gestützt auf die Rückmeldung ergänzt und angepasst.
April-Mai 2005	Analyse und Auswertung der vorliegenden Dokumente und Unterlagen sowie Ausarbeitung des Schlussberichtes durch den EDSB.
23. Mai 2005	Verabschiedung des Schlussberichtes durch den EDSB.

4. Grundlagen des Kontrollberichtes

4.1 Eingereichte Dokumentation / beantwortete Fragen im Vorfeld der Kontrolle

Der Kontrollbericht stützt sich auf die vom MGB eingereichte Dokumentation im Vorfeld der Kontrolle sowie auf die in diesem Zusammenhang ebenfalls beantworteten Fragen des EDSB zu den Datenflüssen und Datenabläufen. Insofern widerspiegelt der Kontrollbericht eine *Bestandesaufnahme* der Datenabläufe, wie sie dem EDSB im Februar 2005 anhand der eingereichten Dokumentation sowie anhand der Besichtigung der Anlagen vor Ort bekannt waren.

M-CUMULUS trägt als erste schweizerische Organisation das Datenschutzgütesiegel GoodPriv@cy, welches Migros von der Schweizerischen Vereinigung für Qualitätsmanagement verliehen wurde. Der EDSB begrüsst es sehr, dass sich die Migros selbstverpflichtend dem Datenschutzgütesiegel unterstellt hat und jährliche Audits durchgeführt werden. Die Datenschutzkontrolle fokussierte sich jedoch auf die Analyse der Datenflüsse im Rahmen des M-CUMULUS-Programms. Da die Aufsichtsfunktion des EDSB im Rahmen der Zertifizierungsverfahren in der laufenden Revision des Datenschutzgesetzes geregelt wird, wurde diese Zertifizierung für die vorliegende Datenschutzprüfung nicht berücksichtigt.

4.2 Kontrolle vom 2. Februar 2005 vor Ort in Zürich

Am 2. Februar 2005 besichtigte der EDSB die Anlagen und Räumlichkeiten der in das CUMULUS-Programm involvierten Akteure am Hauptsitz des MGB in Zürich. Dieser Augenschein vor Ort bildet ebenfalls eine wichtige Grundlage für den vorliegenden Kontrollbericht.

4.2.1 Anwesende Personen

Von Seiten der Migros waren die Datenschutzbeauftragte des MGB, der Leiter M-CUMULUS Direct Marketing, der Leiter Marketing Analysen, die Leiterin der CUMULUS-Infoline sowie der Leiter Data Warehouse Migros IT-Services anwesend. Der EDSB war durch eine Juristische Beraterin sowie einen Informatiker vor Ort vertreten.

4.2.2 Besichtigte Anlagen/Präsentationen

In chronologischer Abfolge:

- Einführung in das M-CUMULUS-Programm
- Besuch des TELAG Call Centers und Besichtigung der Räumlichkeiten der M-CUMULUS Infoline (inkl. Serverraum der TELAG)
- Besichtigung der Räumlichkeiten des Data Warehouse und IT-Services der Migros
- Präsentation der Marketingauswertung im Rahmen von M-CUMULUS
- Besichtigung der Abteilung Marketing Analysen / M-CUMULUS Marketing Services.

4.3 Fact Sheet und beantwortete offene Fragen im Nachgang der Kontrolle

M-CUMULUS hat vom EDSB eine Zusammenstellung der wesentlichen Grundlagen des M-CUMULUS-Programms erhalten, wie es die Mitarbeiter des EDSB gestützt auf die erhaltenen Unterlagen und gestützt auf die Besichtigung vor Ort verstanden haben (sog. Fact Sheet). Dieses Fact Sheet wurde M-CUMULUS Marketing Services und der Rechtsabteilung des MGB zur Konsultation unterbreitet, mit Bitte um materielle Berichtigung. Zusätzlich hat der EDSB von sich aus noch letzte, offene Rückfragen gestellt. M-CUMULUS Marketing Services hat die Änderungswünsche des Fact Sheets mündlich mit dem EDSB besprochen und die Rückfragen schriftlich beantwortet. Das bereinigte Fact Sheet sowie die Antworten auf die Rückfragen stellen ebenfalls eine wichtige Grundlagen für den vorliegenden Kontrollbericht dar.

4.4 Schema der Datenflüsse im Rahmen von M-CUMULUS

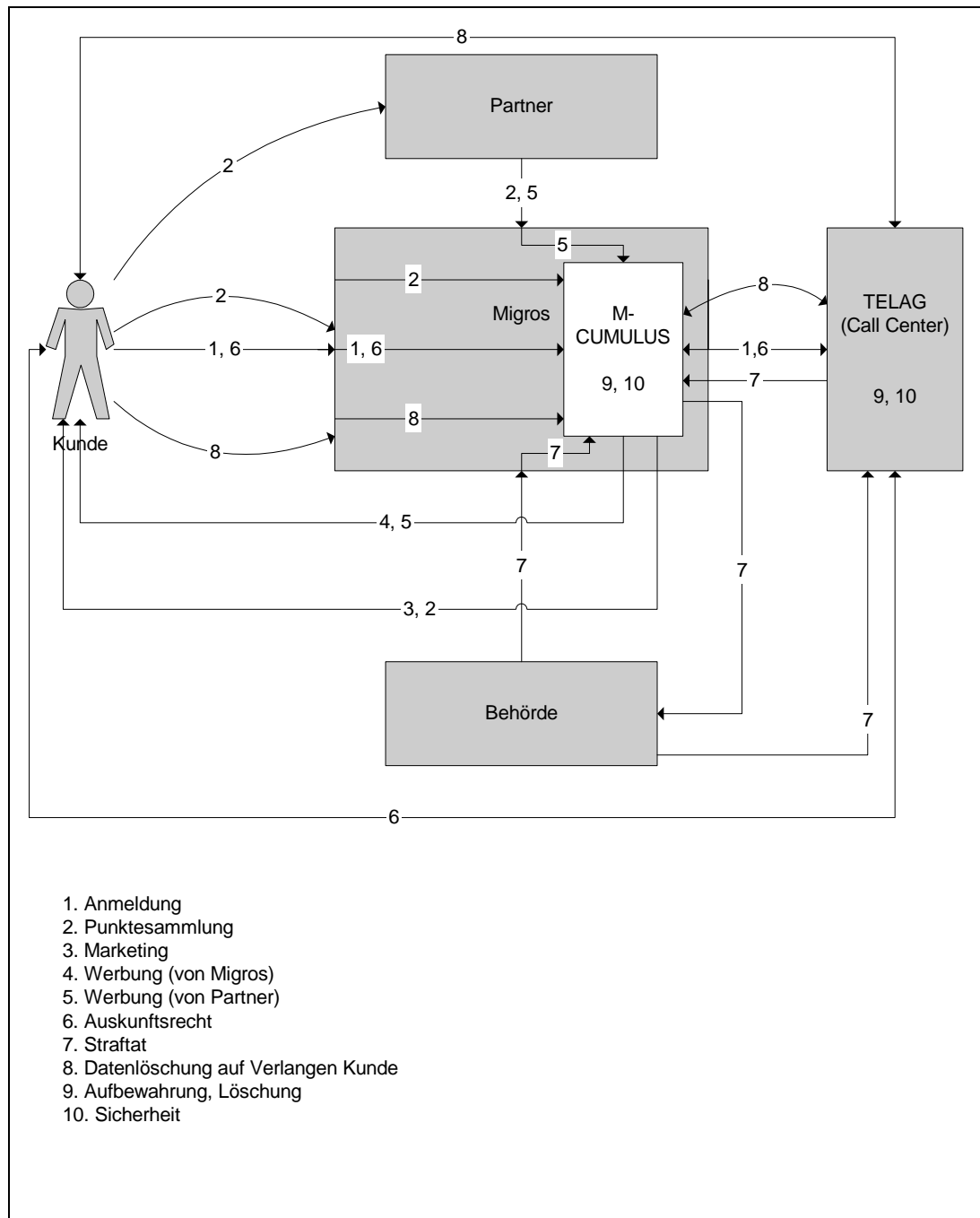
Da die Datenflüsse im Rahmen von M-CUMULUS recht komplex ablaufen, wurden sie vom EDSB in einem Schema „visualisiert“. Dieses Schema wurde zur Überprüfung und mit Bitte um weitere Anregungen an die M-CUMULUS Marketing Services geschickt und nach erfolgter Rückmeldung angepasst.

Das bereinigte Schema liegt dem Kontrollbericht als Basis für die datenschutzrechtliche Beurteilung zugrunde, welche sich an den effektiven Datenflüssen orientiert.

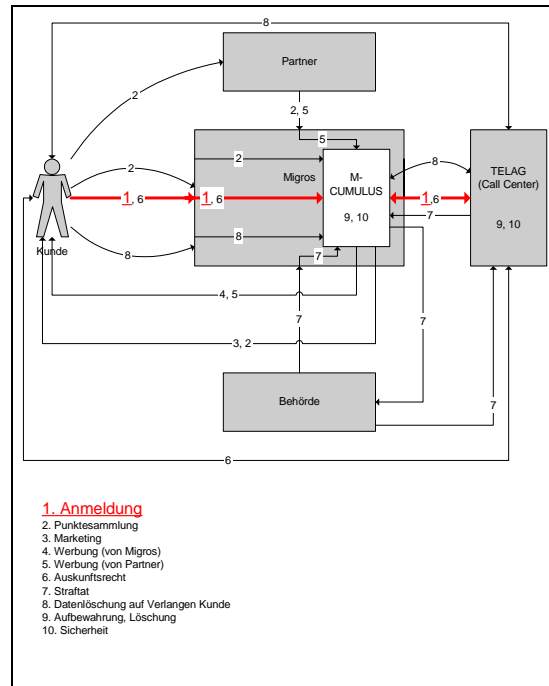
5. Datenschutzrechtliche Beurteilung

Im Folgenden wird das Programm M-CUMULUS einer datenschutzrechtlichen Beurteilung unterzogen. Dafür wird nach den Datenflüssen vorgegangen und die Datenschutzkonformität anhand der einzelnen Abläufe innerhalb des Kundenbindungsprogramms geprüft. Zur Erläuterung und visuellen Darstellung der Datenflüsse wurde folgendes Schema erstellt.

Die Ziffern der einzelnen Datenflüsse innerhalb des Schemas bilden zugleich die Abfolge in der Behandlung der datenschutzrechtlichen Beurteilung.



5.1 Anmeldung



5.1.1 Untersuchte Datenflüsse

Die Anmeldung erfolgt mit einem Anmeldetalon, welcher in jeder Migros-Filiale aufliegt. Der Kunde füllt den Talon mit seinen persönlichen Daten aus und sendet diesen an die Migros. Der Talon wird intern in der Migros an M-CUMULUS weitergeleitet und von dort weiter an das externe Call Center (sog. „CUMULUS-Infoline“; Betreiberin ist die TELAG Communications AG [im Folgenden TELAG]) geschickt, das die Daten in die M-CUMULUS-Datenbank (konkret in das sog. „CuDi“ [=CUMULUS-Dialogsystem; Software-Programm, mit dem alle Stamm- und Programmdateien abrufbar sind]) überträgt.

5.1.2 Anmeldung im Einzelnen

Die Anmeldung zum M-CUMULUS-Programm erfolgt schriftlich durch Ausfüllen des Anmeldetalons in der M-CUMULUS-Broschüre, die in allen Migros-Filialen aufliegt. Die Broschüre enthält detaillierte Angaben zum M-CUMULUS-Programm, eine Auflistung der Programm-Träger und Programm-Partner, bei denen Punkte gesammelt und wieder eingelöst werden können, zwei M-CUMULUS-Karten, 4 Kleber mit der CUMULUS-Nummer, Angaben zur CUMULUS-Infoline und die Allgemeinen Geschäftsbedingungen (im Folgenden AGB).

Obligatorische Angaben auf dem Anmeldetalon sind Name, Anschrift sowie Telefonnummer. E-Mail-Adresse, Geburtsdatum sowie Haushaltsgrösse sind fakultative Angaben und als solches deutlich gekennzeichnet.

Kunden haben auf dem Anmeldetalon die Wahl, vom Angebot auf Direktwerbung zu verzichten (Opting-out). Dieser Verzicht kann jederzeit nachträglich noch geltend gemacht werden (z.B. durch Anruf bei der CUMULUS-Infoline).

Die AGB sind in voller Länge auf der Anmeldebroschüre abgedruckt. Vor kurzem wurde eine ABG-Änderung vorgenommen. Neu wird darauf hingewiesen, dass die Migros die Kundendaten unter Umständen an Dritte weitergeben muss, sofern dies vom geltenden Recht und namentlich von der zuständigen Strafverfolgungsbehörde gefordert wird. Die neuen AGB finden sich auf der Homepage (www.m-cumulus.ch) sowie in den Anmeldebroschüren der West- und italienischen Schweiz. In der Deutschschweiz kommen sie allmählich in Umlauf, da alte Formulare (d.h. Anmeldebroschüren) nicht extra vernichtet, sondern aufgebraucht werden.

Die Anmeldung wird von der TELAG bearbeitet (vgl. zur TELAG Communications AG Ziff. 5.6.2). Die TELAG erfasst die Daten und speichert diese zentral auf dem CUMULUS-Rechner. Die Kartenanträge werden in Heimarbeit erfasst. Die Aufnahme der Daten von neuen CUMULUS-Teilnehmern in den CUMULUS-Kundenstamm erfolgt jeweils am 1. und 15. jedes Monats. Jeweils am 5. und 20. jedes Monats erhalten neue CUMULUS-Kunden einen Begrüssungsbrief.

5.1.3 Beurteilung aus Sicht des EDSB

Mit der Anmeldung zum Kundenbindungsprogramm M-CUMULUS geben die Migros-Kunden auf freiwilliger Basis mit ihrer Einwilligung persönliche Daten (Art. 3 lit. a DSGVO) bekannt und erhalten dafür eine CUMULUS-Nummer, mit der sie von nun an bei jedem Einkauf Punkte sammeln und später einlösen können.

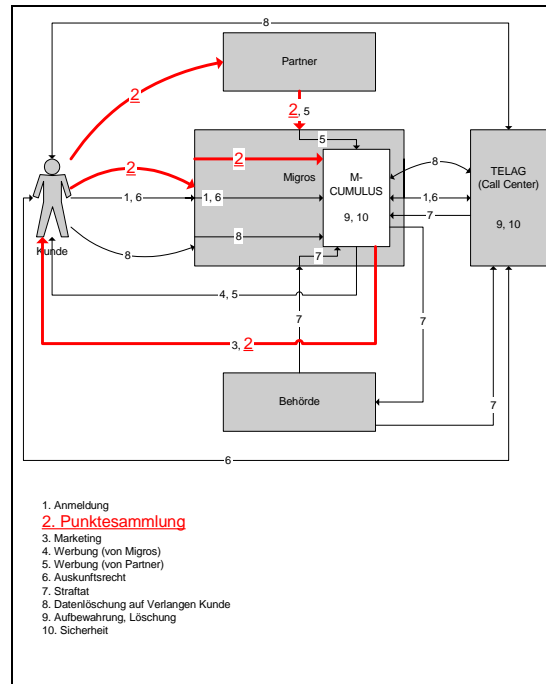
Die mit der CUMULUS-Nummer übermittelten Daten werden von M-CUMULUS für weitere Zwecke bearbeitet. Durch Hinweis auf dem Anmeldebogen und Hinweis in Ziff. 3 der abgedruckten AGB wird auf die Datenbearbeitung hingewiesen. Auch wird in der Anmeldebroschüre explizit aufgeführt, wer Adressen von Kunden beziehen oder verwerten kann, was aus Sicht des Grundsatzes der Transparenz der Datenbearbeitung (Art. 4 Abs. 2 DSGVO) zu begrüssen ist.

Bei der Phase der Anmeldung gibt der Kunde seine Stammdaten in Form von Adressangaben und Telefonnummer bekannt. Alle weiteren Informationen sind rein fakultativ. Bezüglich der Stammdaten erfolgt die Datenerhebung in inhaltlicher Sicht verhältnismässig (Art. 4 Abs. 2 DSGVO).

Die Kunden haben durch Ankreuzen eines entsprechenden Feldes die Möglichkeit, auf weitere Angebote oder Informationen zu verzichten (sog. Opting-out). Ein Kunde hat also die Wahlmöglichkeit, ob er auf weiterführende Angebote und Informationen, konkret Direktwerbung, verzichten möchte (vgl. auch Art. 12 Abs. 2 lit. b DSGVO). Wird das entsprechende Feld nicht angekreuzt, willigt der Kunde implizit in eine weitere Datennutzung seiner Adressdaten ein (Art. 13 Abs. 1 DSGVO).

In der Anmeldebroschüre finden sich umfassende Informationen zum Ablauf und Inhalt des CUMULUS-Programms. Gemeinsam mit den AGB beschreiben diese Angaben den Zweck und Umfang der Datenbearbeitung. Auch in dieser Hinsicht erfolgt die Datenbearbeitung für den Kunden grundsätzlich (vgl. jedoch Ziff. 5.3.3) transparent (Art. 4 Abs. 2 DSGVO).

5.2 Punktesammlung



5.2.1 Untersuchte Datenflüsse

Ein Kunde, der bei einem Programm-Träger oder Programm-Partner einkauft, kann selber entscheiden, ob er seine CUMULUS Karte zeigen will oder nicht. Falls er die Karte vorzeigt, werden ihm die entsprechenden Punkte auf sein Konto gutgeschrieben.

Wenn die Transaktion in einer Migros-Filiale stattgefunden hat, wird die gesamte Transaktion in der CUMULUS-Datenbank gespeichert. Insbesondere werden folgende Informationen festgehalten: *wer* (CUMULUS-Nummer) hat *was* (Warenkorb inkl. detailliertem Inhalt), *wann* (Zeit und Datum) und *wo* (in welcher Filiale) gekauft.

Wenn die Transaktion bei einer Partnerfirma stattfindet, erhält Migros nur eine beschränkte Anzahl von Informationen, und zwar: *wer* (CUMULUS-Nummer) hat *wann* (Zeit und Datum), *wo* (in welcher Filiale) und für *wie viele Punkte* etwas gekauft. Von der Partnerfirma werden in diesem Fall keine Informationen über den Warenkorbinhalt übermittelt.

In periodischen Abständen (alle 2 Monate) erhält ein Kunde eine Abrechnung per Post, auf der sein Punktestand und die gutgeschriebenen CUMULUS-Punkte ersichtlich sind.

5.2.2 Punktesammeln im Einzelnen

Kunden, die am CUMULUS-Programm teilnehmen, können bei jedem Einkauf mit Vorweisen der CUMULUS-Karte Bonus-Punkte sammeln (je 1 Punkt pro 1.- CHF Umsatz). Der Punktestand wird alle zwei Monate zusammengezählt, und pro 500 Punkte erhalten die Kunden per Post einen CUMULUS-Bon im Wert von 5.- CHF. Ab einer gewissen Umsatzgrösse gibt es zusätzliche Treuepunkte. Daneben lanciert Migros regelmässig Bonus-Punkte Aktionen, bei denen mehrfache oder zusätzliche Punkte gesammelt werden können. Das Punktesammeln ist sowohl bei den Programm-Trägern als auch bei gewissen Programm-Partnern möglich.

Damit den Kunden die Bonus-Punkte gutgeschrieben werden können, müssen die gutzuschreibenden Bonus-Punkte zusammen mit der zu begünstigenden CUMULUS-Nummer von den Programm-Trägern oder Programm-Partnern an M-CUMULUS übermittelt werden. Indem er seine CUMULUS-Karte vorzeigt, gibt der Migros-Kunde den Programm-Trägern oder Programm-Partnern die Erlaubnis, die gesammelten Punkte an M-CUMULUS weiterzuleiten. Die Punkte werden über einen Standard Satzaufbau (sog. P004-Record) an M-CUMULUS übermit-

telt. Dieser Standard Satzaufbau muss für jeden Punktelieferanten detailliert festgelegt werden. Der Satzaufbau enthält insbesondere Informationen über Datum, Uhrzeit, Einkaufsbetrag, Einkaufartikel (bei Programm-Trägern), CUMULUS-Nummer, Normalpunkte M-CUMULUS und Aktionspunkte M-CUMULUS.

Beim Programm-Partner Mobility muss die CUMULUS-Nummer bei Vertragsschluss angegeben werden, ansonsten können keine Bonuspunkte gesammelt werden.

Unabhängig vom Punktestand erhalten CUMULUS-Kunden regelmässig Rabatt-Coupons nach Hause geschickt. Die CUMULUS-Kunden können ihre Bons innerhalb der Migros und diversen Migros-Unternehmen gleich wie Bargeld einsetzen.

Wechsel bei den Programm-Partnern sind sehr selten. Deshalb werden den CUMULUS-Teilnehmern diesbezügliche Mutationen vorwiegend über den Werbeversand (z.B. Beilage von Rabatt-Coupons) und sonstige Migros-Publikationen (z.B. Migros-Magazin) angekündigt und nicht in speziellen Mailings. Ob die Kunden ihre CUMULUS-Karte bei einem Einkauf vorweisen oder ihre Rabatt-Coupons bei einem neuen Programm-Partner einlösen wollen, bleibt ihnen überlassen.

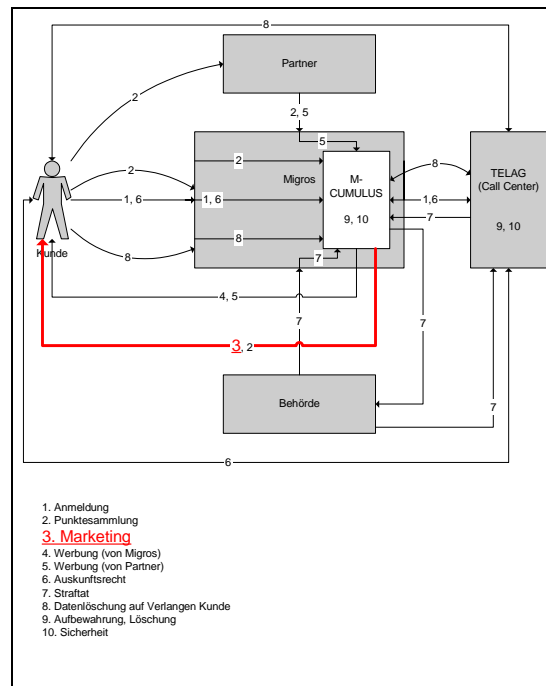
5.2.3 Beurteilung aus Sicht des EDSB

Bonuspunkte können nur gesammelt werden, wenn die betroffene Person ihre CUMULUS-Karte an der Kasse vorweist. Insofern kann die betroffene Person selber bestimmen, wann sie mit ihrem Einkauf Punkte generieren will und wann nicht. Beim Programm-Partner Mobility bedingt das Punktesammeln darüber hinaus die persönliche Angabe der CUMULUS-Nummer auf dem Vertragsformular. Ansonsten reicht es, die CUMULUS-Karte bei einem neuen Partner oder Träger oder bei einem Partner oder Träger, bei dem man noch nie Punkte gesammelt hatte, einfach an der Kasse vorzuweisen. M-CUMULUS gibt von sich aus keine CUMULUS-Nummern an Partner oder Träger heraus. Insofern kann das Kaufverhalten einer Person nicht heimlich oder ohne ihr Wissen festgehalten werden (Datenbearbeitung nach Treu und Glauben, Art. 4 Abs. 2 DSGVO und mit Einwilligung, Art. 13 DSGVO).

Der Datenfluss zwischen den Programm-Trägern oder Programm-Partnern erfolgt per pseudonymisierter CUMULUS-Nummer. Weitere persönliche Daten (wie Name und Personalien) werden im Rahmen der Punktesammlung von den Programm-Trägern oder Programm-Partnern nicht bearbeitet. An dieser Stelle ist hervorzuheben, dass es sich – entgegen der von der Rechtsabteilung MGB vertretenen Meinung – bei der CUMULUS-Nummer um ein Personendatum im Sinne des Art. 3 lit. a DSGVO handelt. Daran ändert auch das Argument nichts, dass den Programm-Trägern und Programm-Partnern die hinter der CUMULUS-Nummer stehenden Personen resp. Adressdaten nicht bekannt sind. Auch wenn nicht bekannt ist, wer die CUMULUS-Karte angemeldet hat, handelt es sich bei der CUMULUS-Nummer um ein Personendatum, welches eine Person bestimmbar macht (vgl. Art. 3 lit. a DSGVO).

Die Datenbearbeitung zwischen den Programm-Trägern und Programm-Partnern und M-CUMULUS erfolgt insofern verhältnismässig (Art. 4 Abs. 2 DSGVO), als in der Regel keine über die CUMULUS-Nummer hinausgehenden Personalien der Betroffenen transferiert werden.

5.3 Marketing



5.3.1 Untersuchte Datenflüsse

Die Abteilung Marketing Analysen kann die M-CULUMUS Daten analysieren, um davon die gewünschten statistischen sowie marketingrelevanten Informationen zu erheben. Mit den Marketingerhebungen kann indirekt auf das Kaufverhalten der Migros-Kundschaft eingewirkt werden, indem z.B. in einer späteren Phase denjenigen CUMULUS-Kunden, welche gewisse Kriterien erfüllen, gezielt Direktwerbung zugesandt wird (vgl. dazu Ziff. 5.4 und 5.5).

5.3.2 Marketing im Einzelnen

Die Einkaufsdaten von CUMULUS-Kunden werden in der CUMULUS-Datenbank festgehalten. In der Abteilung Marketing Analysen haben 6 Mitarbeiter Zugriff auf alle CUMULUS-Daten.

In der Abteilung Marketing Analysen erfolgt die Auswertung der Daten zu Marketing- sowie statistischen Zwecken. Markterhebungen können im TCRM (= Total Customer Relationship Management) bis zum Kauf eines einzigen Produktes vorgenommen werden. Gesucht werden kann also nicht nur nach Produktgruppen, sondern auch nach Einzeleinkäufen. Die Marktanalyse kann z.B. nach Wohnort, Produkt, Alter etc. verfeinert werden. Es gibt auch Erhebungen über die Kaufkraft von Kunden (Einteilung nach sog. Kategorien/Segmenten A-E). In dieser Erhebung werden Kundengruppen gebildet und diese nach Umsatz und Transaktionen eingeteilt. Weiter untersucht werden kann beispielsweise, welches Kundensegment in welchen Fachmärkten einkauft, wie viele Neukunden in einem Jahr hinzugekommen sind, wie effektiv sich Werbemaßnahmen auf Produkte ausgewirkt haben, wie hoch die Wiederkaufsrate bei einem neuen Produkt ist, wie hoch die Rücklaufquote von CUMULUS-Bons ist etc. Die Segmentierung nach Zielgruppen bildet die Entscheidungsgrundlage für spätere Direktwerbung (Direct Marketing) Aktionen (vgl. dazu Ziff. 5.4 und 5.5).

Die Marktanalyse im TCRM und der Vollzugriff auf die CUMULUS-Daten würden es rein theoretisch erlauben, das Kaufverhalten eines einzelnen Kunden zu untersuchen. Jedoch verbietet eine interne Weisung (festgehalten im Datenschutz-Management-Handbuch [im Folgenden DSM-Handbuch]) die Analyse auf Ebene Einzelkunde (also personenspezifisch). Eine solche Analyse auf Ebene Einzelkunde (z.B. im Rahmen einer strafrechtlichen Ermittlung, vgl. unten Ziff. 5.7) muss durch die M-CUMULUS Marketing Services freigegeben werden. In dieser internen Weisung ist auch festgehalten, dass keine Personendaten direkt an irgendwel-

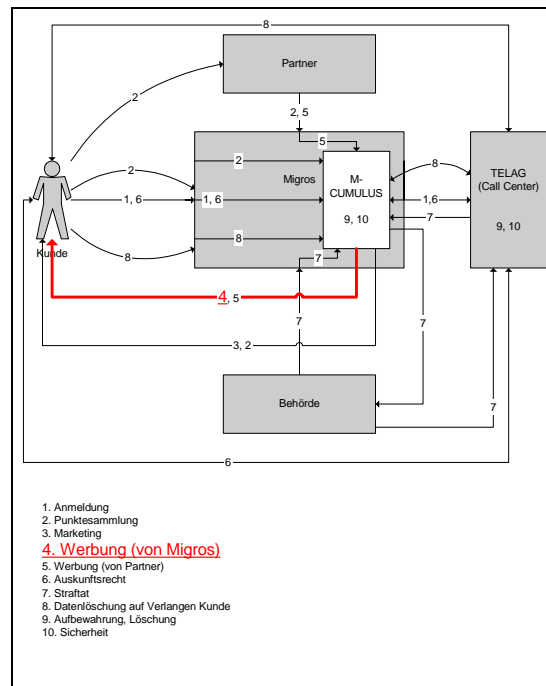
che interne oder externe Interessierte (d.h. an Dritte) oder Auftraggeber (d.h. Trägerunternehmen oder Partnerunternehmen, welche Adressanträge stellen) geliefert werden.

Programm-Träger oder Programm-Partner haben keinen direkten Zugriff auf die CUMULUS-Datenbank. Entsprechende Auswertungsanträge im Hinblick auf Direct Marketing Aktionen laufen immer über die M-CUMULUS Marketing Services (vgl. dazu auch Ziff. 5.4 und 5.5).

5.3.3 Beurteilung aus Sicht des EDSB

Zu den Marketingauswertungen an und für sich gibt es keine Bemerkungen. Jedoch hat sich bei der Datenschutzkontrolle vor Ort herausgestellt, dass im TCRM in Verbindung mit dem CuDi Erhebungen über das Kaufverhalten der CUMULUS-Kundschaft bis zum Kauf eines einzigen Produktes vorgenommen werden können. Gestützt auf die Erhebung von Warenkörben steht der Marketing Abteilung eine enorme Auswahl an Kriterien zur Markt- und Kundenerforschung offen, welche zwar primär pseudonymisiert über die CUMULUS-Nummer erfolgt, jedoch von ihrem Ausmass und ihrer Aussagekraft her weit mehr zulässt, als dies in der Umschreibung in den AGB für die CUMULUS-Kundschaft ersichtlich wird. Aus Sicht des EDSB stellt sich ernsthaft die Frage, ob sich die CUMULUS-Kundschaft der Datenbearbeitung ihrer Warenkörbe in diesem Ausmass genügend bewusst ist und sie insbesondere genügend darüber informiert ist. Aus Sicht des EDSB besteht bei der Aufklärung der CUMULUS-Kundschaft hier eine Informationslücke, welche von M-CUMULUS durch eine bessere Information und Zweckumschreibung der Datenbearbeitung in den AGB behoben werden muss.

5.4 Werbung (von Migros)



5.4.1 Untersuchte Datenflüsse

Die Abteilung Marketing Analysen kann im Auftrag von M-CUMULUS Marketing Services die Daten von CUMULUS-Kunden analysieren und gestützt darauf kundenspezifische Werbung (Direct Marketing Aktionen) lancieren. Die Auswahlkriterien der Marketinganalysen für diese sog. Direktwerbung können sehr variabel sein (z.B. Kaufkraft, Umsatz, Wohnort, Alter, Kaufgruppe eines bestimmten Produktes oder Produktsortiments). Die von den CUMULUS-Kunden erhaltenen und gesammelten Daten erlauben eine detaillierte Warenkorbanalyse. Mit den gewählten Kriterien wird eine gewisse Gruppe von Kunden ausgewählt und gezielt angeschrieben. Die Adressen werden von einer Druckerei (im Folgenden Mailhouse oder Lettershop genannt) ausgedruckt und die Werbung direkt an die einzelnen Haushalte verschickt.

5.4.2 Werbung im Einzelnen

Jeder aktive Teilnehmer am M-CUMULUS-Programm erhält 6x im Jahr (also alle 2 Monate) eine persönliche Kontoabrechnung mit den ihm zustehenden CUMULUS-Bons und weiteren Rabatt-Coupons. Ebenso wird jedem aktiven Teilnehmer die Broschüre „Migros Special“ zugestellt (sofern die Broschüre im Versandmonat gedruckt wurde, was nicht immer der Fall ist). Die Broschüre Migros Special (z.B. vom März 2005 zum Thema „Baby“) wird dabei gezielt an diejenigen Kunden verschickt, welche in der Abrechnungsperiode aus einem bestimmten Produktsortiment (z.B. Baby-Artikel) Artikel gekauft haben. Adressdaten für den „CUMULUS-Versand“ gehen direkt von IT-CUMULUS an die Migros-internen Document Services zur Weiterverarbeitung.

Auf Wunsch der einzelnen Migros-Genossenschaften verschickt M-CUMULUS sog. „Aktuell“-Seiten mit lokalen Inhalten. Diese werden auch an Kunden geschickt, welche keine Werbung wünschen.

Kunden, die vom Angebot weiterreichender Angebote oder Informationen Gebrauch machen möchten, erhalten mit dem 2-monatlichen Versand weitere, einkaufspezifische Werbung. Die Marketingabteilung von M-CUMULUS betreibt Direktwerbung primär für Unternehmen, die zur Migros Gemeinschaft gehören (d.h. für die Unternehmen, die zum MGB gehören, wie Migros-Filialen, OBI, Hotelplan, Micasa, sportXX, M-Electronics etc.). Alle hausinternen Anfragen für einkaufspezifische Angebote laufen über die M-CUMULUS Marketing Services.

Ein hausinterner Versand läuft z.B. wie folgt ab: Die Produktverantwortlichen von Migros setzen die Ziele fest, für was und für welches Kundensegment man Direktwerbung betreiben will (z.B. für bestimmte Baby-Artikel; Personen mit einer bestimmter Postleitzahl; die 100 Kunden, welche im Bereich Kaffee in der Abrechnungsperiode den grössten Umsatz erzielt haben). Diese Auswertung und die entsprechende Suche der Adressen dieser CUMULUS-Kunden läuft über die Abteilung Marketing Analysen im Auftrag der M-CUMULUS Marketing Services (vgl. dazu auch oben, Ziff. 5.3.2).

Bei Direktwerbung wird immer angegeben, dass man aufgrund der M-CUMULUS-Teilnahme mit den vorliegenden Werbeinfos bedient wird. Das muss aus dem Versand klar hervorgehen und wird durch die M-CUMULUS Marketing Services kontrolliert. Die M-CUMULUS Marketing Services achten auch darauf, dass die Kunden keine „Werbeflut“ nach Hause geschickt erhalten. Wenn zu viele Anfragen von Produktverantwortlichen nach Direktwerbung vorliegen, wird sondiert.

Der grösste Teil an einkaufsspezifischen Versänden wird ausserhalb der 2-monatlichen Abrechnungsperiode lanciert. Auch bei diesem Versand muss immer klar hervorgehen, dass man aufgrund der Teilnahme am M-CUMULUS-Programm angeschrieben wurde. Der Werbeversand ausserhalb der 2-monatlichen Abrechnungsperiode muss darüber hinaus mit einem „Vorteil/Mehrwert“ für die angeschriebenen Kunden verbunden sein (z.B. Einladung zu einem Eröffnungsapéro; weitere Rabattgutscheine).

Alle Anträge für Direktwerbung müssen an die M-CUMULUS-Marketing Services gestellt werden. Diese prüfen, ob die Selektionskriterien sinnvoll gewählt wurden und ob nicht schon zu viele Werbesendungen in einer gewissen Zeitspanne verschickt wurden. Bei Gutheissung des Versandes werden die gewünschten Kundenadressen in der Regel nicht direkt an die Programm-Träger herausgegeben. Vielmehr werden die sondierten Adressen von M-CUMULUS Marketing Services gemeinsam mit dem Werbematerial an ein Mailhouse resp. Lettershop (bei Eigenpressebeilagen an die Limmatdruck AG) weitergeleitet, wo der Versand gedruckt wird (inkl. Adressen). Die Adressen werden also immer der Stelle zur Verfügung gestellt, welche sie auch verarbeitet. In den wenigsten Fällen ist der Besteller der Adressen auch der Verarbeiter (Ausnahmen z.B. bei kleineren Mailings, vgl. gleich weiter unten).

Die Kundendaten werden von M-CUMULUS Marketing Services an ein Mailhouse resp. Lettershop (Limmatdruck AG oder anderer externer Verarbeiter) übermittelt. Die Übermittlung erfolgt für kleine Datenmengen via verschlüsselter Emails, für grosse Datenmengen via CD-Rom mit verschlüsselten Dateien. Mit Unterschrift auf dem Lieferschein bestätigen die Adressempfänger (Mailhouse/Lettershop), dass sie die Daten nach der Verwendung löschen oder an die M-CUMULUS Marketing Services zurückschicken.

Möglich ist auch, dass Produkte zurückgerufen werden müssen. Auch hier erfolgt die Anschrift der Kunden über die CUMULUS-Datenbank (wer hat das Produkt in der fraglichen Zeit gekauft). Auch die Aufträge für einen Produktrückruf und damit verbunden die Adressherausgabe laufen über die M-CUMULUS Marketing Services.

Bei kleinen Mailings (d.h. Mails, bei denen z.B. nur 100 Personen angeschrieben werden, wie die besten 100 Kunden von sportXX) werden die Adressen direkt dem Programm-Träger herausgegeben (nicht jedoch den Programm-Partnern; diese erhalten Adressdaten nie direkt).

Diejenigen Firmen der Migros-Gemeinschaft, welche Adressen beziehen können, sind in der Anmeldebroschüre namentlich unter dem Titel „Datenschutz konkret“ erwähnt (MGB, Migros-Genossenschaften, sportXX, DO IT + GARDEN, Micasa, OBI, Forissimail, Migros-Online-Shopping, Saisonküche, Migros-Klubschule, Migros-Freizeitzentren, Golf Parcs, Hotelplan, Eurocentres, MIGROSBANK, Ex Libris, Migrol).

Auf der Anmeldebroschüre kann fakultativ die Email-Adresse angegeben werden. Genutzt wurden die Email-Adressen erst einmalig für einen Werbeversand von Florissimail. Die Bestellung und Herausgabe der Email-Adressen läuft nach den gleichen Vorgaben, wie oben umschrieben (d.h. insbesondere über die M-CUMULUS Marketing Services).

5.4.3 Einige Zahlen zum Versand von Direktwerbung

Die folgenden Zahlen wurden dem EDSB von der M-CUMULUS Marketing Services zur Verfügung gestellt:

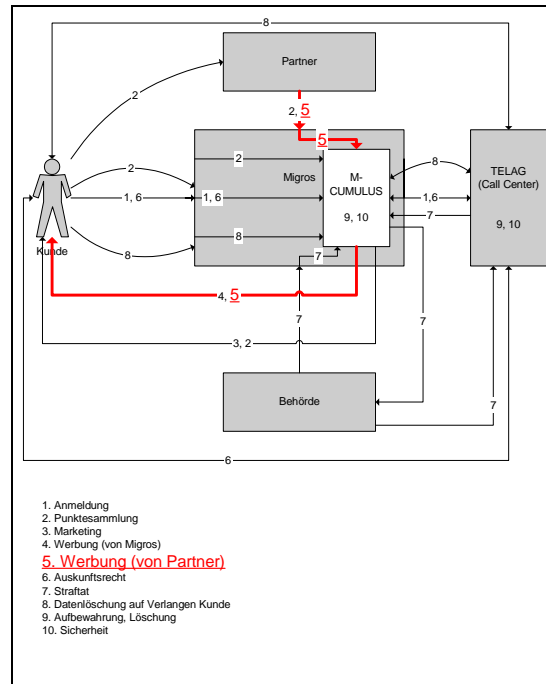
- *Anzahl Werbeversand im Jahr 2004:*
 Durchgeführte Mailings und Eigenpressebeilagen: 95 (inkl. 6 CUMULUS-Versände)
 Davon für Partner (Generali; vgl. dazu auch Ziff. 5.5.2): 13
- *Quantität der Mailings:*
 Die Zielgruppe wird für jedes Mailing neu zusammengesetzt. Viele Mailings erfolgen in kleinen Mengen. Gemäss Auskunft der M-CUMULUS Marketing Services sind deshalb Mehrfachbelieferungen von Kunden resp. Adressüberschneidungen gering.
- *Maximale Mailingmenge:*
 Die Portokosten limitieren die Direktwerbung auf eine Auflage von max. 200'000 Exemplare. Grössere Zielgruppen werden mit selektiven Eigenpressebeilagen bedient. Die Auflagen bewegen sich dort bis zu ca. 1,5 Mio. Exemplare.

5.4.4 Beurteilung aus Sicht des EDSB

Mit der Anmeldung am CUMULUS-Programm willigt ein Kunde explizit ein, dass seine CUMULUS-Daten zu Marketingzwecken ausgewertet werden. Wer keine zusätzlichen Informationen oder Angebote erhalten will, kann dies mit einer Verzichtserklärung in der Anmeldung zum Ausdruck bringen. In Ziff. 12 der AGB heisst es, dass Migros ihrer CUMULUS-Kundschaft periodisch spezielle CUMULUS-Angebote unterbreitet. Im Zusammenhang mit der Möglichkeit der Verzichtserklärung geht man als Kunde wohl davon aus, dass man neben der Abrechnung und den CUMULUS-Bons sowie Rabatt-Coupons kein weiteres Werbematerial erhält. Bezüglich des Versandes der „Aktuell“-Seiten an Kunden, die keine Werbung wünschen, besteht hier eine Lücke in der Aufklärung gegenüber der CUMULUS-Kundschaft. Es erscheint aus Sicht des EDSB fraglich, ob dieser Werbeversand von der Einwilligung der CUMULUS-Kunden (Art. 13 DSGVO), gerade im Hinblick auf die Möglichkeit der Verzichtserklärung, gedeckt ist.

Demgegenüber ist es auch Sicht des EDSB zu begrüssen, dass auf die Möglichkeit der Adressnutzung explizit in der Anmeldebroschüre hingewiesen wird und diejenigen Migros-Unternehmen, welche Adressen (z.T. auch direkt) verwenden und beziehen dürfen, namentlich erwähnt werden. Dies trägt zur Transparenz der Datenbearbeitung (Art. 4 Abs. 2 DSGVO) bei. Ebenso zu begrüssen ist die Tatsache, dass jeder Versand von Direktwerbung mit einem Vorteil für die CUMULUS-Kundschaft verbunden sein muss und alle Adressanträge für entsprechende Versände von der Abteilung M-CUMULUS Marketing Services gutgeheissen werden müssen (Grundsatz der inhaltlichen Verhältnismässigkeit resp. Datensparsamkeit, Art. 4 Abs. 2 DSGVO). Hervorzuheben ist auch die Tatsache, dass Adressdaten nie an Partnerunternehmen direkt herausgegeben werden und damit das Risiko einer Zweckentfremdung (vgl. Art. 4 Abs. 3 DSGVO) möglichst gering gehalten wird.

5.5 Werbung (von Partnern)



5.5.1 Untersuchte Datenflüsse

Die Partner von Migros können ebenfalls die M-CULUMUS-Daten für gezielte Werbung nutzen. Bei der Nutzung der CUMULUS-Daten fließen jedoch keine Kundendaten (Personalien/Einkaufsdaten) von M-CUMULUS zu den Partnerunternehmen. Vielmehr kann ein Partner die gewünschte Zielgruppe beschreiben, und den Auftrag an M-CUMULUS weitergeben. Die M-CUMULUS Marketing Services werden das Adress- und Werbegesuch prüfen, bei Gutheissung die entsprechenden Kundenadressen der gewünschten Zielgruppe auswählen lassen (von Abteilung Marketing Analysen) und den Kunden die von den Partnerfirmen gelieferte Werbung senden (via Mailhouse resp. Lettershop).

5.5.2 Werbung von Partnern im Einzelnen

Direktwerbung für Partnerunternehmen wird sehr selten betrieben. Bis heute erfolgte ein solcher Werbeversand einzig für Generali. Hier wurden Kunden mit einem bestimmten Alter (ausgewertet nach dem freiwillig offenbarten Geburtsdatum) angeschrieben.

Auch bei einem (allfälligen) Werbeversand für Partnerunternehmen werden nur diejenigen Kunden angeschrieben, welche vom Angebot weiterreichender Informationen oder Angebote Gebrauch machen möchten. Der Ablauf gestaltet sich ähnlich wie oben unten Ziff. 5.4.2 umschrieben. So ist ebenfalls vorausgesetzt, dass die angeschriebenen Kunden informiert sind, woher ihre Adressen stammen. Zusätzlich muss auch hier immer ein Vorteil/Mehrwert (wie Rabatt-Coupons; Einladung zum Eröffnungsapéro) dem Versand beigelegt oder gewährt werden. Auch bei einem solchen Versand läuft die Adressanfrage über die M-CUMULUS-Marketing Services. Die von Partnerunternehmen erfragten Adressen werden den Partnerunternehmen nie direkt herausgegeben, sondern werden chiffriert (vgl. oben Ziff. 5.4.2) an ein Mailhouse (Limmatdruck AG oder externer Verarbeiter) weitergeleitet.

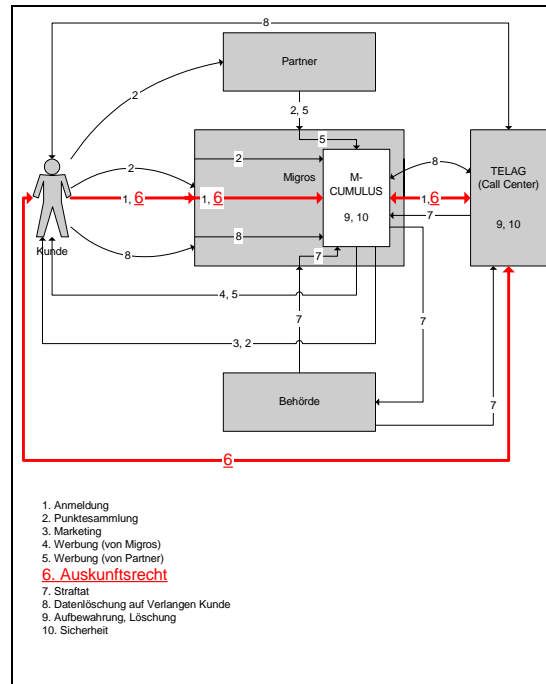
5.5.3 Beurteilung aus Sicht des EDSB

Ein Werbeversand für Partnerunternehmen gestützt auf CUMULUS-Daten ist bis anhin erst einmalig durchgeführt worden. Ein entsprechender Antrag muss ebenfalls immer von der M-CUMULUS Marketing Services gutgeheissen werden. Den Partnerunternehmen werden die sondierten Adressdaten der CUMULUS-Kundschaft nie direkt ausgehändigt. Insofern er-

scheint im Hinblick auf die Adressherausgabe und im Hinblick auf den Werbeversand die inhaltliche Verhältnismässigkeit der Datenbearbeitung resp. der Grundsatz der Datensparsamkeit (Art. 4 Abs. 2 DSGVO) gewährleistet. Zusätzlich wird vertraglich klargestellt, dass M-CUMULUS den Partnerunternehmen keine Personalien der CUMULUS-Kundschaft und insbesondere auch keine Kundenadressen oder andere Informationen über die CUMULUS-Kunden zur Verfügung stellt (Ziff. 4 des CUMULUS-Partner-Vertrages). Diese Vertragsklausel dient ebenfalls der Gewährleistung der inhaltlichen Verhältnismässigkeit der Datenbearbeitung (Art. 4 Abs. 2 DSGVO) und tritt der Gefahr einer Zweckentfremdung (vgl. Art. 4 Abs. 3 DSGVO) durch Migros-externe Partnerunternehmen entgegen.

Für die CUMULUS-Kundschaft hingegen ist die Möglichkeit der indirekten Datennutzung durch Partnerunternehmen für gezielte Direktwerbung wenig ersichtlich. Weder in der Informationsbroschüre noch in den AGB wird auf diese (wenn auch indirekte) Adressnutzung hingewiesen. Zwar wird bei einem solchen Werbeversand immer explizit darauf hingewiesen, dass die Adressen von M-CUMULUS stammen, dennoch erhält der Kunde gestützt auf sein individuelles Kaufverhalten oder sonstiger persönlicher Begebenheiten Werbematerial eines externen Partnerunternehmens. Da Direktwerbung für Partnerunternehmen bis anhin eher selten betrieben wurde, erscheint diese Informationslücke nicht gravierend. Sollte in Zukunft in Betracht gezogen werden, für Partnerunternehmen vermehrt gezielte Direktwerbung zu betreiben, drängt sich hier aus Sicht des EDSB eine Präzisierung in der Anmeldebroschüre oder den beigelegten AGB auf.

5.6 Auskunftsrecht



5.6.1 Untersucher Datenfluss

Ein Kunde kann sein datenschutzrechtlich garantiertes Recht auf Auskunft (Art. 8 DSGVO) geltend machen, indem er entweder das Call Center (CUMULUS-Infoline resp. TELAG) oder den MGB direkt kontaktiert. Ferner hat er die Möglichkeit, seinen Punktestand und sein Kundenkonto per Internet abzufragen.

5.6.2 Auskunftsrecht im Einzelnen

Die CUMULUS-Infoline wird von der „TELAG Communications AG“ (Sitz in Zürich) betrieben. Die TELAG beschäftigt in ihren Räumlichkeiten 25-30 Personen für die CUMULUS-Infoline. Auf der Anmeldebroschüre sowie auf der Website von M-CUMULUS wird ausdrücklich auf die Infoline hingewiesen (Telefon- und Faxnummer; Email-Adresse; www-Adresse). Auf eine ausdrückliche Erwähnung des Auskunftsrechtes wurde in den AGB verzichtet. Gemäss Aussage der Datenschutzbeauftragten des MGB ergibt sich das Auskunftsrecht bereits aus Art. 8 DSGVO und muss daher in den AGB nicht mehr speziell erwähnt werden.

Kleine Auskunftsgesuche über einzelne Einkäufe (z.B. verlorene Kassensbons mit CUMULUS-Nummer für Garantie-Fälle auf Produkte) können telefonisch gestellt werden. Die TELAG schickt in diesem Fall einen Auszug des konkreten Einkaufs, ohne dass dies schriftlich bestellt werden muss. Ohne grössere bürokratische Hürden wird in diesen Fällen ein Auszug des Kassensbeleges herausgegeben. Solche Auskunftsgesuche können nur von 3 Personen bei der TELAG ausgedruckt und bearbeitet werden. Alle weiteren Mitarbeiter haben keinen Druckeranschluss. Es bestehen schriftliche Anweisungen (DMS-Handbuch) für die Bearbeitung von mündlichen Auskunftsbegehlen. Diese Anweisungen liegen dem EDSB vor.

Grössere Auskunftsbegehlen müssen an die M-CUMULUS Marketing Services weitergeleitet werden. Nur sie haben die Kompetenz, solche Gesuche zu beantworten. Dies läuft dann nicht direkt über die TELAG, sondern über die Migros selber. Die Kunden müssen dazu ein schriftliches Formular ausfüllen und unterschreiben, welches sie von der TELAG zugeschickt bekommen. Die Mitarbeiter von TELAG haben in diesen Fällen strikte Vorgehensanweisungen (im DMS-Handbuch festgehalten). Dem auskunftssuchenden Kunden wird ein standardisierter Begleitbrief und ein standardisiertes Antragsformular zugestellt. Die Kunden können Auskünfte verlangen über „Personalien und Programmsteuerungs-Informationen“, „Einkaufsdaten (Kassenzetteltotal pro Einkauf inkl. Datum)“ oder „Einkaufsdaten (Kassenzetteltotal pro

Einkauf inkl. Datum, inkl. einzelne eingekaufte Produkte)“. Zudem kann der Kunde die Periode bestimmen, innerhalb derer er Auskunft über die Daten wünscht. Von den Kunden wird nicht verlangt, dass sie sich mit der Kopie eines amtlichen Ausweises identifizieren. Alle beantragten und eingegangenen Auskunftsbegehren werden im CuDi vermerkt. Bis heute sind Auskunftsersuchen (auch vollumfassende, über Jahre hinaus gehende) gratis.

Ein Kunde hat zudem die Möglichkeit, sich jederzeit mündlich bei der CUMULUS-Infoline über seinen aktuellen Punktestand zu informieren.

Die M-CUMULUS Marketing Services ist nicht darüber informiert, wie das Auskunftsrecht über gesammelte CUMULUS-Daten bei Partnerfirmen gehandhabt wird. Die auskunftssuchenden Kunden werden aber im 2. Begleitschreiben, in denen sie die gewünschten Daten erhalten, darauf aufmerksam gemacht, dass die CUMULUS-Nummer verknüpft mit Einkaufsdaten ebenfalls bei Generali, der Migrosbank oder anderen Programmpartnern gespeichert sein könnte.

Die CUMULUS-Kundschaft hat auch die Möglichkeit, per Internet Einblick in ihre CUMULUS-Daten zu erhalten. Per Internet können die Personalien, der kumulative Einkaufsbetrag und die kumulative Punktezahl der laufenden Periode sowie ein Abbild der Kontoauszüge der letzten drei Abrechnungsperioden (PDF) eingesehen werden. Ersichtlich sind per Internetabfrage keine Warenkörbe, sondern eine Auflistung der generierten Punkte bei Programm-Trägern oder Programm-Partnern. Ein Kunde kann direkt Änderungen an seinen Stammdaten (mit Ausnahme von Vor- und Nachnamen) durchführen. Die Internetabfrage läuft per Login mit der CUMULUS-Nummer und einem eigenen oder von der Migros zur Verfügung gestellten Passwort. Die Abfrage erfolgt chiffriert (https-Verbindung). Die im Internet zur Verfügung gestellten CUMULUS-Daten werden nicht in einer Zwischendatenbank gespiegelt (tägliches Update).

Gemäss Aussagen der M-CUMULUS Marketing Services wird das Auskunftsrecht von der CUMULUS-Kundschaft nur selten in Anspruch genommen.

5.6.3 Beurteilung aus Sicht des EDSB

Das Auskunftsrecht der betroffenen Personen gegenüber dem Dateninhaber einer Datensammlung gehört zu den zentralen Elementen des Datenschutzrechts. Der Dateninhaber hat gegenüber der auskunftssuchenden Person alle Angaben offen zu legen, die sich auf diese Person beziehen und in einer Datensammlung enthalten sind (Art. 8 Abs. 1 und 2 DSGVO), wobei die Identität des Gesuchstellers durch den Dateninhaber zu überprüfen ist (Art. 1 Abs. 1 der Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 [SR 235.11; VDSG]).

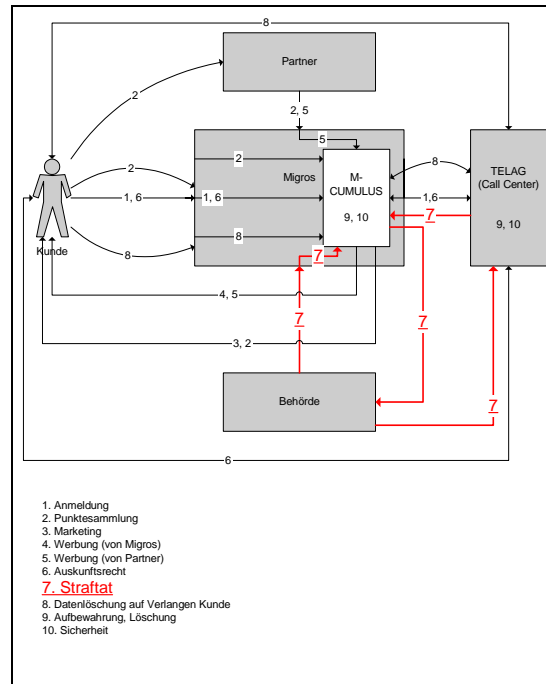
Ein CUMULUS-Kunde kann sich über die CUMULUS-Infoline jederzeit über den aktuellen Kontostand informieren, so ist es in den AGB (Ziff. 7) festgehalten. Die Nummer der Infoline ist sowohl in Ziff. 6 der AGB als auch in der Anmeldebroschüre unterhalb der AGB abgedruckt. Wie bereits von den beiden Mitarbeitern des EDSB vor Ort angeregt wurde, stellt sich die Frage, ob auf das Auskunftsrecht nicht deutlicher in den AGB hingewiesen werden sollte. Die zuständige Datenschutzbeauftragte des MGB vertrat damals den Standpunkt, dass das Auskunftsrecht gesetzlich bereits in Art. 8 DSGVO festgehalten sei und deshalb keine spezielle Erwähnung in den AGB finden müsse. Der EDSB regt jedoch an, dass das Auskunftsrecht deutlicher in den AGB zum Ausdruck kommen sollte. Dies rechtfertigt sich zum einen aus der Sensibilität der von M-CUMULUS bearbeiteten Personendaten (Einkaufsdaten des Warenkorbes; widerspiegelt Konsumverhalten der Betroffenen). Zum anderen hat sich der MGB Anfang dieses Jahres dazu entschlossen, die CUMULUS-Kundschaft in den AGB auf die Möglichkeit der Datenweitergabe an Strafverfolgungsbehörden hinzuweisen (vgl. dazu die Bemerkungen in Ziff. 5.1.2 und Ziff. 5.7), auch wenn diese Pflicht zur Datenherausgabe bereits auf Gesetzesstufe geregelt ist.

Zur Gewährung des Auskunftsrechtes wird von der antragstellenden Person keine Kopie eines amtlichen Ausweises verlangt. Jedoch besteht nur ein geringes Missbrauchsrisiko, da Auskunftsbegehren (mit Ausnahme von kleinen Kassenbon-Auszügen) schriftlich gestellt werden müssen. Die Kunden, welche sich telefonisch mit der CUMULUS-Infoline in Verbindung setzen, erhalten ein Formular nach Hause geschickt, das sie anschliessend ausfüllen und unterzeichnen müssen. Durch das standardisierte Formular und dessen direkter Zustellung zum Karteninhaber ist ein unberechtigter Zugriff auf die CUMULUS-Daten über das Auskunftsrecht kaum denkbar.

Ein CUMULUS-Kunde kann sein Recht auf Auskunft auch über Internet ausüben. Mittels CUMULUS-Nummer und Passwort (eigenes oder von Migros gestelltes) kann ein Kunde seine Personalien sowie seinen (aktuellen oder vergangenen) Punktesaldo abrufen. Zusätzlich kann der Kunde von sich aus per Internet seine Stammdaten ändern (mit Ausnahme von Vor- und Nachname). Die Kontoabfrage per Internet erfolgt chiffriert, was unter dem Aspekt der Datensicherheit (Art. 7 DSGVO) zu begrüssen ist.

Der EDSB ist darüber erstaunt, dass die CUMULUS-Kundschaft selten von ihrem Auskunftsrecht Gebrauch macht. Gemäss Auskunft der M-CUMULUS Marketing Services werden Auskunftsgesuche eher selten gestellt.

5.7 Datenauskünfte bei einer Straftat



5.7.1 Untersucher Datenfluss

Falls Behörden im Rahmen einer (Straf-)Untersuchung Informationen über CUMULUS-Kunden brauchen, müssen sie sich an die Rechtsabteilung des MGB wenden. Anfragen über die CUMULUS-Infoline oder an den MGB werden an M-CUMULUS weitergeleitet. Wenn die Anfrage auf Datenherausgabe gerechtfertigt ist (in Absprache mit der Rechtsabteilung des MGB), liefert M-CUMULUS die gefragten Informationen (typischerweise handelt es sich bei diesen Informationen um die Personalien des Kontoinhabers, welche gestützt auf eine bekannte CUMULUS-Nummer auffindig gemacht werden).

5.7.2 Weiterleitung von Kundendaten bei Straftaten im Einzelnen

Als Grundlage dienen M-CUMULUS die einschlägigen Textpassagen in den Tätigkeitsberichten des EDSB. Die Daten werden ausschliesslich dann herausgegeben, wenn Migros gegenüber den zuständigen Behörden zeugnispflichtig ist. Entsprechend werden keine Daten an die Polizei herausgegeben. Gemäss Auskunft der Datenschutzbeauftragten MGB und M-CUMULUS Marketing Services wird selbst der zuständigen Strafverfolgungsbehörde gegenüber nur dann Auskunft über CUMULUS-Daten erteilt, wenn intern die Verhältnismässigkeit der Datenherausgabe geprüft wurde.

In diversen Fällen, welche alle dokumentiert sind, wurden im Rahmen einer konkreten Ermittlung CUMULUS-Daten (Personalien) an die zuständige Strafuntersuchungsbehörde geliefert. Dabei ging es meist um sog. „Güsel-Sünder“.

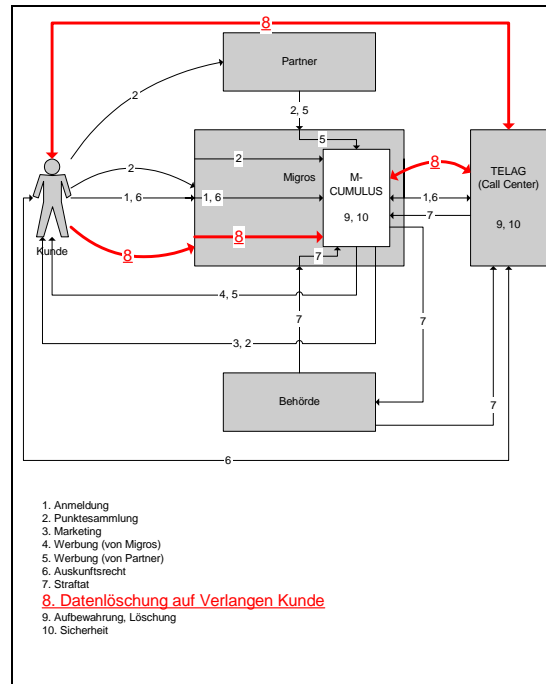
Aktuelle Zahlen für das Jahr 2004 betreffend Datenherausgabe an Dritte (Behörden etc.):

- *Anfragen / Betroffene Personen (Total):* 213
 - Anzahl Personen, deren Personalien an Dritte herausgegeben wurden (meist Güsel-Sünder): 177
 - Anzahl Personen, deren Personalien nicht an Dritte herausgegeben wurden: 36

5.7.3 Beurteilung aus Sicht des EDSB

Anfang dieses Jahres hat der MGB eine Änderung der CUMULUS-AGB vorgenommen. Neu wird explizit darauf hingewiesen, dass die Migros die Kundendaten unter Umständen an Dritte weitergeben muss, sofern dies vom geltenden Recht und namentlich von der zuständigen Strafverfolgungsbehörde gefordert wird (vgl. dazu auch die Ausführungen in Ziff. 5.1.2). Eine Datenherausgabe wird immer anhand des Einzelfalles auf ihre Verhältnismässigkeit überprüft. Beide Massnahmen (Erwähnung in AGB und Einzelfallprüfung) sind auch Sicht des EDSB sehr zu begrüessen.

5.8 Datenlöschung auf Verlangen der Kunden



5.8.1 Untersucher Datenfluss

Ein Kunde kann von sich aus die Löschung seiner Daten verlangen und damit aus dem CUMULUS-Programm aussteigen. Löschanträge können an die Migros resp. M-CUMULUS oder an die TELAG resp. das Call Center gerichtet werden. Die Löschanträge werden vom Call Center bearbeitet und M-CUMULUS übermittelt.

5.8.2 Löschanträge im Einzelnen

Verlangt ein CUMULUS-Kunde die Löschung seiner Daten, so werden diese nicht allesamt gelöscht, sondern anonymisiert. Die Löschung bezieht sich nur auf die im Antragsformular angegebenen Stammdaten. Die Programmdateien stehen also weiterhin für statistische Zwecke zur Verfügung.

Der Kunde muss einen Löschantrag schriftlich an M-CUMULUS stellen. Er kann den Löschauftrag auch mündlich via Call Center deponieren, jedoch kann diese Löschung nicht gestützt auf mündliches Begehren ausgeführt werden. Die Mitarbeiter des TELAG Call Centers haben in diesem Fall strikte Vorgehensanweisungen (festgehalten im DMS-Handbuch) der M-CUMULUS Marketing Services, welche sie zu befolgen haben. Bei mündlichen Löschanträgen erhält der Kunde vom Call Center ein standardisiertes Begleitschreiben sowie ein entsprechendes Formular mit Löschantrag nach Hause geschickt, das dieser auszufüllen und zu unterzeichnen hat. Die Beilage einer Kopie eines amtlichen Ausweises wird nicht verlangt.

Im Begleitschreiben wird der Kunde ausdrücklich darauf aufmerksam gemacht, dass sich die Löschung auf seine Stammdaten im operativen CUMULUS-System bezieht und ein Abbild der abgerechneten Kontoauszüge auf CD-Rom erhalten bleibt, mit der jedoch keine Datenbearbeitungen mehr vorgenommen werden. Ebenso wird der Kunde darauf hingewiesen, dass er alle auf sein Konto laufende CUMULUS-Karten und CUMULUS-Etiketten vernichten soll, damit z.B. nicht andere Haushaltsmitglieder weiterhin auf diese Karte CUMULUS-Punkte sammeln. CUMULUS-Karten können nicht gesperrt werden.

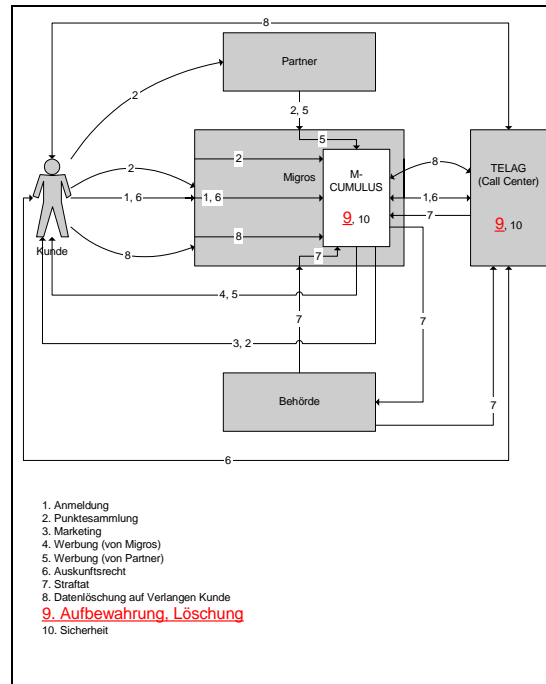
5.8.3 Beurteilung aus Sicht des EDSB

Ebenso wie das Auskunftsrecht gehört auch das Löschungsrecht zu den fundamentalen Rechtsgewährleistungen des Datenschutzrechtes. Ein Kunde kann verlangen, dass seine personenbezogenen Daten für keine weiteren Datenbearbeitungen mehr zur Verfügung stehen. Daher ist das Löschungsrecht aus Sicht des EDSB in den AGB explizit aufzuführen (vgl. auch die entsprechenden Bemerkungen in Ziff. 5.6.2). Die Mitarbeiter des EDSB hatten bereits bei der Besichtigung der Anlagen vor Ort darauf aufmerksam gemacht. Ebenso wurde von den Mitarbeitern festgestellt, dass bei verlorengegangenen Karten keine Kartensperrung möglich ist. Ein Kunde hat hingegen jederzeit die Möglichkeit, bei einer abhanden gekommenen Karte die Löschung des CUMULUS-Kontos in Auftrag zu geben, was zur Missbrauchsvermeidung eine ausreichende Schutzmassnahme darstellt.

Im standardisierten Löschformular von M-CUMULUS findet sich jedoch eine unklare Aussage, welche bereinigt werden sollte. Es wird im Löschauftrag folgender Satz verwendet: „Als Inhaber/in des CUMULUS-Konto mit folgender Nummer beauftrage ich MGB beziehungsweise M-CUMULUS, folgendes Konto zu löschen“. Gemäss dem Wortlaut geht der Kunde also davon aus, dass seine gesamten Konto-Daten gelöscht werden. Die Löschung bezieht sich aber tatsächlich nur auf die Stammdaten. Die Programmdateien werden anonymisiert und sind zu statistischen Zwecken weiterhin zugänglich. Dies sollte im Löschauftrag klargestellt werden.

Mit der Löschung der Personalien auf Begehren eines Kunden werden die in der CUMULUS-Datenbank festgehaltenen Daten anonymisiert und können keiner bestimmten oder bestimmbarer Person mehr zugeordnet werden. Das DSGVO findet daher auf die Bearbeitung dieser anonymisierten Daten keine Anwendung mehr.

5.9 Aufbewahrung und Löschung weiterer Daten



5.9.1 Untersucher Datenfluss

Innerhalb des M-CUMULUS-Programms wird mit verschiedenen Personendaten operiert. Für deren Aufbewahrung und Löschung gelten unterschiedliche Regeln. Die Aufbewahrungsfristen sind alle im DMS-Handbuch umschrieben. Dem EDSB liegt die entsprechende Auflistung vor.

5.9.2 Aufbewahrung und Löschung weiterer Daten im Einzelnen

Die Anmeldetalons der CUMULUS-Kundschaft werden bei der TELAG gesammelt und dort in einem Entsorgungscontainer aufbewahrt. Die Talons werden dort ca. alle 6 Wochen vernichtet (max. Aufbewahrungszeit beträgt 2 Monate).

Auskunftsbegehren, Löschaufträge sowie alle weitere Kundenkorrespondenz der M-CUMULUS Marketing Services oder der TELAG werden für 2 vergangene Kalenderjahre aufbewahrt.

Adressänderungen, gefundene CUMULUS-Karten oder Postretouren werden max. 2 Monate bei der TELAG im Entsorgungscontainer aufbewahrt.

Die gelieferten Rohdaten von Partnerunternehmen („P004“Lieferant + CUMULUS-Nummer) werden zwischen 4 bis max. 10 Monaten aufbewahrt. P004 Rohdaten für das CUMULUS-Dialogsystem CuDi bleiben länger bestehen.

Kontobewegungen bleiben während max. 3 Jahren im CuDi. Löschungen werden jährlich im Januar für die Daten durchgeführt, die älter als 2 Jahre sind. Detail- d.h. Produktdaten (Warenkörbe) verschwinden nach 15 Monaten.

Die Einkaufsdaten der CUMULUS-Teilnehmer werden nach 15 Monaten gelöscht (weil Computerkapazität hier an Grenzen stösst).

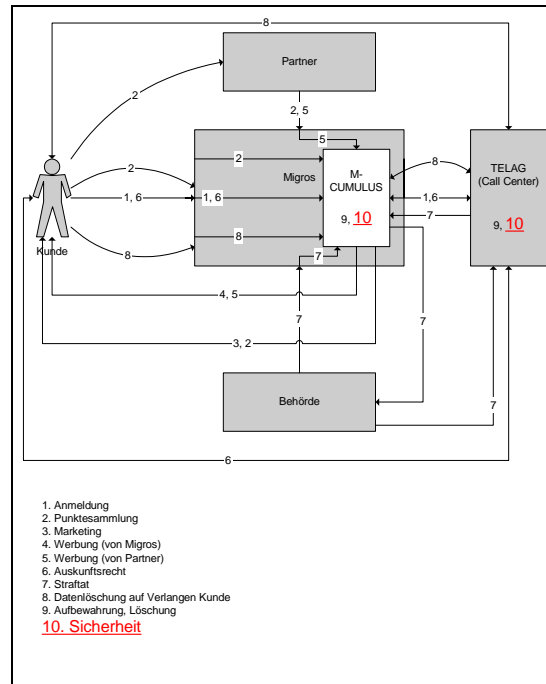
Die Kassenbons selber werden nach Vorgabe des Obligationenrechts für 10 Jahre aufbewahrt (geschäftsrelevante Unterlagen).

5.9.3 Beurteilung aus Sicht des EDSB

Die Rohdaten sind datenschutzrelevant. Eine Transaktion eines Partnerunternehmens mit Einkaufsort, Einkaufsdatum, Einkaufstotal in CHF sowie CUMULUS-Nummer enthält Personendaten, da gestützt auf die CUMULUS-Nummer der Karteninhaber bestimmbar ist (vgl. auch die entsprechende Bemerkung in Ziff. 5.2.3). Es handelt sich hier um pseudonymisierte Daten, nicht anonymisierte Daten. Aus diesem Grund ist die Aussage, wie sie im DSM-Handbuch festgehalten ist, falsch, dass die Aufbewahrung der Rohdaten P004 keine Datenschutzrelevanz habe.

Die Aufbewahrungsdauer stellt aus Sicht des EDSB eine relevante Information für den Kunden, der sein Einkaufsverhalten gegenüber Migros offen legt, dar. Aus diesem Grund regen wir an, dass in den AGB ein Vermerk aufgenommen wird, dass die im Rahmen des CUMULUS-Programms erhobenen Daten bis zu 3 Jahre aufbewahrt werden. Zusätzlich sollten für den Kunden die relevanten Aufbewahrungsfristen im Internet abrufbar aufgeführt werden.

5.10 Sicherheit³



5.10.1 Untersuchte Räume

(...)

5.10.2 Sicherheitsmassnahmen im Einzelnen

(...)

5.10.3 Beurteilung aus Sicht des EDSB

(...)

³ Aufgrund überwiegender Interessen der Migros an der Vertraulichkeit dieser Angaben wurden die entsprechenden Passagen zur Datensicherheit (gesamte Ziff. 5.10) für die Publikation aus dem Bericht herausgenommen. Die Datenschutzkontrolle des EDSB hat gezeigt, dass die Sicherheitsmassnahmen **den Anforderungen des Datenschutzgesetzes entsprechen**.

5.11 Sensibilisierung und Schulung von CUMULUS-Mitarbeitern

5.11.1 Ergriffene Massnahmen

M-CUMULUS Marketing Services stellen sicher, dass alle Personen, welche innerhalb des MGB auf die CUMULUS-Datenbank Zugriff haben, eine „Geheimhaltungserklärung“ unterzeichnen. Grundsätzlich wird darauf geachtet, dass nur diejenigen Personen mit den persönlichen CUMULUS-Kundendaten in Kontakt kommen, welche auch funktional damit zu tun haben. Dieser kleine Kreis von Mitarbeitern (ca. 11 Mitarbeiter) wird von der Datenschutzbeauftragten des MGB jährlich in Sachen Datenschutz geschult und sensibilisiert. Neue Mitarbeiter erhaltenen auch ausserhalb der jährlichen Schulungen ein persönliches Briefing durch die Datenschutzbeauftragte des MGB. Dem EDSB liegt ein Schulungsplan vor. Die Mitarbeiter von M-CUMULUS haben jederzeit die Möglichkeit, mit der Datenschutzbeauftragten des MGB Kontakt aufzunehmen, wenn datenschutzrechtliche Fragen oder Unklarheiten auftreten. Diese Kontaktaufnahme ist gratis, d.h. dass die Mitarbeiter dafür kein Visum der vorgesetzten Person brauchen und auch sonst keine Hürden überwinden müssen.

Die Mitarbeiter des TELAG Call Centers, welche Zugriff auf das CuDi haben (ca. 25-30 Personen), werden im Rahmen ihrer Ausbildung durch die TELAG selbst auf Datenschutzfragen geprüft (Fachkompetenz-Prüfung; Schulungshandbuch) und unterzeichnen eine Datenschutzerklärung, welche für alle angebotenen Auskunftsdienste der TELAG die gleiche Erklärung ist. Des Weiteren werden die Mitarbeiter der Infoline alle 2 Monate durch die Datenschutzbeauftragte des MGB in Sachen Datenschutz geschult und sensibilisiert. So wissen etwa die Mitarbeiter, dass sie aus dem CuDi nur bestimmte Auskünfte und diese auch nur den Karteninhabern erteilen dürfen. Die Einhaltung dieser Regeln wird durch die Migros Datenschutzstelle regelmässig (anhand fiktiver Anrufe) überprüft.

Weiter bestehen interne Weisungen, welche die erlaubten Aktivitäten für jede mit CUMULUS-Daten involvierte Abteilung (M-CUMULUS Marketing Services; Marketing Analysen; IT-CUMULUS) umschreiben. Diese Weisungen liegen dem EDSB vor.

5.11.2 Beurteilung aus Sicht des EDSB

Der EDSB begrüsst das Schulungskonzept und die Sensibilisierungsmassnahmen des MGB im Rahmen von M-CUMULUS sehr und hat dazu keine weiteren Bemerkungen.

6. Ergebnisse

Aufgrund der Auswertung der eingereichten Unterlagen und Dokumente sowie gestützt auf die durchgeführte Kontrolle vom 2. Februar 2005 gemäss Art. 29 DSG, gelangt der EDSB zu einer durchwegs **positiven Gesamtbeurteilung**. Die Datenschutzkontrolle hat gezeigt, dass die im Rahmen von M-CUMULUS vorgenommene Datenbearbeitung **grundsätzlich datenschutzkonform** verläuft. Trotz dieser überwiegend positiven Beurteilung ist der EDSB in seiner Datenschutzkontrolle auch auf Sachverhalte gestossen, welche aus datenschutzrechtlicher Sicht einer **Anpassung resp. Änderung bedürfen**.

Ausgehend von diesem Gesamtbild erlässt der EDSB zuhanden des MGB mit Sitz in Zürich seine Gesamtbeurteilung in folgender Form:

- **Feststellungen;**
- **Anpassungs- resp. Verbesserungsvorschläge; oder**
- **Empfehlungen im Sinne des Art. 29 Abs. 3 DSG.**

6.1 Anmeldung

Die Transparenz (Art. 4 Abs. 2 DSG) bei der Anmeldung zum Kundenbindungsprogramm M-CUMULUS ist für die Teilnehmer weitgehend gewährleistet (zum Hauptkritikpunkt siehe Ziff. 5.3.3). Positiv zu bewerten sind insbesondere die ausführlichen Informationen über das Programm in der Anmeldebroschüre sowie die darauf ebenfalls vollständig abgedruckten AGB. Die Datenerhebung bei der Anmeldung hält vor dem Grundsatz der inhaltlichen Verhältnismässigkeit (Art. 4 Abs. 2 DSG) stand. Dem Kunden bleibt bei der Anmeldung sowie während der gesamten Dauer der Teilnahme am Kundenbindungsprogramm die Wahlmöglichkeit, auf weitergehende Direktwerbung zu verzichten.

6.2 Punktesammlung

Es werden nur dann personenbezogene Daten erhoben, wenn ein Kunde seine CUMULUS-Karte beim Verbuchen des Einkaufs vorzeigt. Ein Kunde kann also ganz bewusst auch auf die Erhebung seiner Daten bei gewissen Einkäufen verzichten. Des Weiteren ist ein Kunde der Migros nicht auf den Besitz der CUMULUS-Karte angewiesen, um gewisse Produkte günstiger zu erhalten. Es besteht also eine Wahlmöglichkeit resp. ein Alternativverhalten aus Sicht der Kundschaft.

6.3 Marketing

Die erhobenen Personendaten sind weitgehend mit einer zugeordneten CUMULUS-Nummer pseudonymisiert. *Der EDSB möchte an dieser Stelle jedoch noch einmal klarstellen, dass auch die pseudonymisierte CUMULUS-Nummer ein Personendatum darstellt, auf das die Datenschutzprinzipien anwendbar sind.* M-CUMULUS als DateninhaberIn, hat über die Verknüpfung der CUMULUS-Nummer mit den Personalien Zugriff auf Einkaufsdaten der DateninhaberIn. Irrelevant ist aus Sicht des EDSB das von der Migros vorgebrachte Argument, dass CUMULUS-Karten von mehreren Personen gebraucht werden können. Nichtsdestotrotz wird bei M-CUMULUS mit Personendaten (z.B. über das Konsumverhalten) operiert, welche einer Person (KarteninhaberIn) zugeordnet werden können.

Auch wenn das Kundenbindungsprogramm vorwiegend über die pseudonymisierte CUMULUS-Nummer abläuft, werden hier vom MGB personenbezogene Daten bearbeitet, welche

dem Schutz des DSGVO unterstehen und für deren datenschutzkonforme Bearbeitung (auch durch externe Stellen) der MGB die Verantwortung trägt.

Die im Rahmen von M-CUMULUS erhobenen Personendaten können durch die Abteilung Marketing Analysen zu Marketingzwecken ausgewertet werden. In den AGB wird darauf hingewiesen, und die CUMULUS-Kunden willigen in diese Datenbearbeitung ein. Bei der Datenschutzkontrolle vor Ort hat sich herausgestellt, dass im TCRM Erhebungen über das Kaufverhalten der CUMULUS-Kundschaft bis zum Kauf eines einzigen Produktes vorgenommen werden können. Gestützt auf die Erhebung von Warenkörben steht der Marketing Abteilung eine enorm grosse Auswahl von Kriterien zur Markt- und Kundenerforschung offen, welche zwar primär pseudonymisiert über die CUMULUS-Nummer erfolgt, jedoch von ihrem Ausmass und ihrer Aussagekraft her weit mehr zulässt, als dies in der Umschreibung in den AGB für die CUMULUS-Kundschaft ersichtlich wird (vgl. Ziff. 5.3.2).

Empfehlung Nr. 1:

Der EDSB erlässt die Empfehlung, dass die Zweckumschreibung bezüglich der Warenkorbanalysen und Marketingauswertungen in den AGB präziser und für den Kunden transparenter formuliert wird: „Sie erlauben der Migros, Informationen über Ihre Einkäufe zu sammeln und zu Marketingzwecken auszuwerten. Gestützt auf Ihre Einkaufsdaten können Warenkorbanalysen durchgeführt werden, welche das Konsumverhalten sowie persönliche Kundenprofile widerspiegeln.“ (Ziff. 3 AGB).

6.4 Werbung (von Migros)

CUMULUS-Kunden erhalten trotz der Erklärung, dass sie auf weitere Informationen und Angebote der Migros oder deren Partner verzichten möchten, „Aktuell“-Seiten der einzelnen Migros-Genossenschaften mit lokalen Inhalten zugeschickt. In Ziff. 12 der AGB heisst es, dass Migros ihrer CUMULUS-Kundschaft periodisch spezielle CUMULUS-Angebote unterbreitet. Im Zusammenhang mit der Möglichkeit der Verzichtserklärung muss ein CUMULUS-Kunde hingegen davon ausgehen können, dass er neben der Abrechnung und den CUMULUS-Bons sowie Rabatt-Coupons kein weiteres Werbematerial erhält. Es besteht hier eine Lücke in der Aufklärung gegenüber der CUMULUS-Kundschaft. Es erscheint aus Sicht des EDSB fraglich, ob dieser Werbeversand von der Einwilligung der CUMULUS-Kunden (Art. 13 DSGVO) gedeckt ist.

Empfehlung Nr. 2:

Der EDSB erlässt die Empfehlung, dass entweder in der Anmeldebroschüre oder den AGB auf diesen Spezialversand hingewiesen wird, oder dass dieser Versand in Zukunft ganz unterlassen wird.

Der Versand von Direktwerbung bei denjenigen Kunden, welche weitere Informationen und Angebote erhalten möchten, erfolgt transparent und in inhaltlicher Hinsicht verhältnismässig (Art. 4 Abs. 2 DSGVO). Alle Adressanträge für Werbeversände laufen über die M-CUMULUS Marketing Services und müssen von dieser Abteilung gutgeheissen werden. Der EDSB hat bezüglich der Direktwerbung durch Unternehmen der Migros-Gemeinschaft keine weiteren Bemerkungen.

6.5 Werbung (von Partnern)

Für externe Programmpartner wird kaum Direktwerbung betrieben, und sollte dies doch der Fall sein, so werden Adressdaten nie an die Partnerunternehmen herausgegeben. Vertraglich abgesichert ist ferner, dass M-CUMULUS den Partnerunternehmen keine Personalien der CUMULUS-Kunden und insbesondere keine Kundenadressen oder andere Informationen über die CUMULUS-Kunden zur Verfügung stellt. Dadurch wird auch die Gefahr der Zweckentfremdung (vgl. Art. 4 Abs. 3 DSGVO) und das Missbrauchspotenzial minimiert. Im Bereich der Direktwerbung besteht eine Informationslücke bezüglich der indirekten Adressnutzung durch Partnerunternehmen. Weder in der Informationsbroschüre noch in den AGB wird darauf hingewiesen, dass ein Kunde gestützt auf sein Kaufverhalten oder sonstiger persönlicher Begebenheiten via M-CUMULUS Werbematerial von Partnerunternehmen erhält.

Anpassungs-/Verbesserungsvorschlag Nr. 1:

Sollte von der Migros in Zukunft in Betracht gezogen werden, im Rahmen von M-CUMULUS für Partnerunternehmen vermehrt gezielte Direktwerbung zu betreiben, so sind aus Sicht des EDSB dahingehende Präzisierungen in den AGB und in der Anmeldebroschüre vorzunehmen.

6.6 Auskunftsrecht

Grundsätzlich hat ein CUMULUS-Kunde ausreichend die Möglichkeit, in Erfahrung zu bringen, welche Daten über ihn im Rahmen von M-CUMULUS bearbeitet werden. Kleinere Auskunftsgesuche, z.B. zur Geltendmachung von Garantiefällen, werden ohne grössere bürokratische Hürden von der TELAG mündlich entgegengenommen und erledigt. Darüber hinausgehende Auskunftsgesuche müssen schriftlich gestellt werden. Dafür werden den antragstellenden Personen standardisierte Formulare nach Hause geschickt. Dadurch wird auch das Missbrauchsrisiko eingedämmt. In einfacherer Form kann ein Kunde sein Auskunftsrecht auch selbst per Internetabfrage (CUMULUS-Nummer und Passwort) ausüben.

Anpassungs-/Verbesserungsvorschlag Nr. 2:

Trotz dieser positiven Bewertung des Auskunftsrechtes schlägt der EDSB vor, dass in den AGB explizit auf das Auskunftsrecht hingewiesen wird. Diese Anregung wurde bereits bei der Kontrolle vor Ort von den anwesenden Mitarbeitern des EDSB vorgebracht. Eine höhere Transparenz beim Auskunftsrecht rechtfertigt sich aus Sicht des EDSB gestützt auf die Tatsache, dass im Rahmen des Kundenbindungsprogramms M-CUMULUS mit sensiblen Personendaten umgegangen wird und hier deshalb die Kunden besser über ihr Auskunftsrecht aufzuklären sind.

Ein CUMULUS-Kunde kann sein Recht auf Auskunft auch über Internet ausüben. Mittels CUMULUS-Nummer und Passwort (eigenes oder von Migros gestelltes) kann ein Kunde seine Personalien sowie seinen (aktuellen oder vergangenen) Punktesaldo abrufen. Zusätzlich kann der Kunde per Internet seine Stammdaten ändern (mit Ausnahme von Vor- und Nachname). Die Kontoabfrage per Internet erfolgt chiffriert. Gemäss Auskunft von M-CUMULUS Marketing Services soll es in Zukunft auch möglich sein, über den aktuellen Punktesaldo hinaus den eigenen Warenkorb per Internet einzusehen.

6.7 Datenauskünfte bei Straftaten

CUMULUS-Daten werden an aussenstehende Behörden nur dann herausgegeben, wenn die Migros gegenüber den zuständigen Behörden zeugnispflichtig ist. Entsprechend werden keine Daten an die Polizei herausgegeben. Die Datenherausgabe bei einer Straftat wird immer einer Einzelfallprüfung unterzogen und auf ihre Verhältnismässigkeit hin überprüft. Diese zusätzliche Einzelfallprüfung ist aus Sicht des EDSB zu begrüssen.

6.8 Datenlöschung auf Verlangen der Kunden

Ein Kunde kann auf eigenes Verlangen seine Stammdaten löschen lassen. Die Löschung muss mit einem standardisierten Formular eingefordert werden, welches dem Karteninhaber persönlich nach Hause geschickt wird. Auch hier wird dadurch das Missbrauchspotenzial eingedämmt.

Anpassungs-/Verbesserungsvorschlag Nr. 3:

Vermehrt noch als beim Auskunftsrecht drängt sich beim Löschungsrecht eine explizite Erwähnung in den AGB auf. Der EDSB regt an, dass dies vom MGB so umgesetzt wird.

Im standardisierten Löschformular von M-CUMULUS findet sich eine unklare Aussage, welche ebenfalls bereinigt werden sollte. Es wird im Löschauftrag folgender Satz verwendet: „Als Inhaber/in des CUMULUS-Konto mit folgender Nummer beauftrage ich MGB beziehungsweise M-CUMULUS, folgendes Konto zu löschen“.

Anpassungs-/Verbesserungsvorschlag Nr. 4:

Gemäss dem Wortlaut geht der Kunde also davon aus, dass seine gesamten Konto-Daten gelöscht werden. Die Löschung bezieht sich aber tatsächlich nur auf die Stammdaten. Die Programmdateien werden anonymisiert und sind zu statistischen Zwecken weiterhin zugänglich. Dies sollte im Löschauftrag klargestellt werden.

6.9 Aufbewahrung und Löschung weiterer Daten

Bei der Übermittlung von Rohdaten durch Partnerunternehmen handelt es sich aus Sicht des EDSB um pseudonymisierte Personendaten, deren Bearbeitung ebenfalls datenschutzrelevant ist. Der EDSB unterstreicht diese Tatsache und fordert die verantwortlichen Personen des CUMULUS-Programms auf, sich dieser Tatsache bewusster zu sein. Die Aufbewahrungsdauer der im Rahmen von M-CUMULUS erhobenen Personendaten stellt aus Sicht des EDSB eine relevante Information für die CUMULUS-Kundschaft dar.

Anpassungs-/Verbesserungsvorschlag Nr. 5:

Der EDSB fordert den MGB daher auf, dass in den AGB ein Vermerk aufgenommen wird, dass die im Rahmen des CUMULUS-Programms erhobenen Daten bis zu 3 Jahre aufbewahrt werden. Zusätzlich sollten für den Kunden relevante Aufbewahrungsfristen umschrieben werden und die Fristen im Internet abrufbar aufgeführt werden.

Die Aufbewahrungsfristen im Einzelnen erscheinen dem EDSB verhältnismässig.

6.10 Sicherheit⁴

(...)

Anpassungs-/Verbesserungsvorschlag Nr. 6:

(...)

(...)

6.11 Sensibilisierung und Schulung von CUMULUS-Mitarbeitern

Der EDSB begrüsst das Schulungskonzept und die Sensibilisierungsmassnahmen des MGB im Rahmen von M-CUMULUS sehr und regt an, diese auch in Zukunft so weiterzuführen.

6.12 Datentransfer ins Ausland

Im Nachgang der Kontrolle vor Ort vom 2. Februar 2005 wurde dem EDSB schriftlich gemäss Art. 6 DSG ein Datentransfer ins Ausland gemeldet. Der EDSB begrüsst diese Anmeldung.

Anpassungs-/Verbesserungsvorschlag Nr. 7:

Darüber hinaus schlägt der EDSB vor, dass die Datenübermittlung mit Erwähnung des Destinationslandes in die AGB aufgenommen wird.

⁴ Aufgrund überwiegender Interessen der Migros an der Vertraulichkeit dieser Angaben wurden die entsprechenden Passagen zur Datensicherheit (gesamte Ziff. 6.10) für die Publikation aus dem Bericht herausgenommen. Die Datenschutzkontrolle des EDSB hat gezeigt, dass die Sicherheitsmassnahmen **den Anforderungen des Datenschutzgesetzes entsprechen**.

7. Schlussfolgerungen

7.1 Bezüglich der Kontrolle des Kundenbindungsprogramms M-CUMULUS

Im Rahmen des Kundenbindungsprogramms M-CUMULUS werden Personendaten von einem Grossteil der Schweizer Bevölkerung (es bestehen mehr als 2 Mio. CUMULUS-Konten) bearbeitet. Die durchgeführte Datenschutzkontrolle konnte dem EDSB einen vertieften Einblick in die Abwicklung und in die Datenflüsse im Rahmen von M-CUMULUS liefern. Die von der Migros zur Verfügung gestellten Unterlagen und Dokumentationen haben es dem EDSB erlaubt, die im Rahmen von M-CUMULUS vollzogene Bearbeitung von Personendaten einer vertieften Prüfung und detaillierten Analyse zu unterziehen und damit die Einhaltung der Datenschutzbestimmungen zu überprüfen.

Dem EDSB hat sich ein überwiegend positives Gesamtbild der Datenbearbeitung präsentiert. Wo Anpassungs- oder Änderungsbedarf besteht, hat dies der EDSB mit Begründung erläutert.

7.2 Verfahren und weiteres Vorgehen

Im Rahmen des Kundenbindungsprogramms M-CUMULUS werden seit dem 1. November 1997 grosse Mengen Kundendaten erfasst und zu Marketing- sowie statistischen Zwecken ausgewertet. Gestützt auf die dem EDSB vorliegenden Zahlen – die M-CUMULUS-Datenbank führt mehr als 2 Millionen Kundenkonten – kann davon ausgegangen werden, dass sich das Kundenbindungsprogramm in den letzten 7 Jahren etabliert hat und von einem Grossteil der Schweizer Bevölkerung in Anspruch genommen wird. In Anbetracht des grossen Benutzerkreises und der Sensibilität der bearbeiteten Personendaten erwies sich die nun erstmalig erfolgte umfassende Überprüfung von M-CUMULUS bezüglich der Einhaltung der Datenschutzbestimmungen als sehr aufschlussreich und bedeutungsvoll.

Aus besagten Gründen besteht ein grundsätzliches Interesse daran, die Öffentlichkeit für diese Art der Datenerhebung zu sensibilisieren und sie insbesondere über die erfolgte Datenschutzkontrolle bei M-CUMULUS und die diesbezüglichen Ergebnisse zu informieren. Gestützt auf Art. 30 Abs. 2 DSG wird der EDSB daher den vorliegenden Kontrollbericht betreffend das Kundenbindungsprogramm M-CUMULUS in einer angepassten Version (und bezüglich Namensnennungen anonymisiert) der Öffentlichkeit zugänglich machen und ihn *auf seiner Website* (www.edsb.ch) *publizieren*. Selbstverständlich erfolgt die Publikation unter dem Vorbehalt, dass keine aus Sicht des MGB vertraulichen Daten, welche Geschäftsgeheimnisse offenbaren oder die Konkurrenzfähigkeit beeinflussen könnten, bekannt gegeben werden. Der MGB (Zürich) wird daher aufgefordert, den Kontrollbericht auf solche vertraulichen Inhalte hin zu überprüfen und dem EDSB **mit Frist von 30 Tagen** entsprechend schriftliche Rückmeldung zu erstatten.

Der vorliegende Kontrollbericht enthält eine Reihe von *Feststellungen* sowie *Anpassungs- resp. Verbesserungsvorschläge*, welche vom EDSB auf Basis der durchgeführten Kontrolle verfasst wurden. Der MGB wird gebeten, vorliegenden Kontrollbericht sowie die darin enthaltenen Feststellungen und Vorschläge zur Kenntnis zu nehmen und dem EDSB **mit Frist von 30 Tagen** darüber zu informieren, ob von Seiten des MGB irgendwelche *Bemerkungen* dazu vorliegen und ob, und wenn ja, *mit welchen Massnahmen* und *innerhalb welcher Frist* die Vorschläge des EDSB umgesetzt werden.

Darüber hinaus enthält der vorliegende Kontrollbericht *Empfehlungen* im Sinne des Art. 29 Abs. 3 DSG, welche sich an den Migros-Genossenschafts-Bund MGB, Limmatstrasse 152, Postfach, 8031 Zürich, richten. Der MGB teilt dem EDSB **mit Frist von 30 Tagen** mit, *ob* er diese Empfehlungen *akzeptiert oder nicht*. Falls die Empfehlungen abgelehnt oder nicht befolgt werden, kann der EDSB die Angelegenheit der Eidgenössischen Datenschutzkommission zum Entscheid vorlegen (Art. 29 Abs. 4 DSG).

Bern, den 23. Mai 2005

**EIDGENÖSSISCHER
DATENSCHUTZBEAUFTRAGTER**

Der Beauftragte:

Hanspeter Thür

Anhang vom 28. September 2005 zum Schlussbericht

1. Vorbemerkung

Der vorliegende Anhang widerspiegelt die Stellungnahmen von Seiten der Migros auf den Schlussbericht vom 23. Mai 2005 des EDSB. Die Stellungnahmen wurden dem EDSB fristgerecht innerhalb von 30 Tagen am 21. Juni 2005 eingereicht. Nach eingehender Prüfung der Stellungnahmen hat der EDSB die Antworten und Vorschläge von Migros ausgewertet und seinerseits schriftlich am 2. August 2005 darauf reagiert. Die Reaktionen des EDSB sowie die letzten Stellungnahmen von Migros datierend vom 8. August 2005 sind ebenfalls in vorliegendem Anhang wiedergegeben. Der Anhang bildet integralen Bestandteil des Schlussberichtes.

Der EDSB hat am 28. September 2005 die Datenschutzkontrolle gemäss Art. 29 DSGVO über das Kundenbindungsprogramm M-CUMULUS für abgeschlossen erklärt.

2. Auswertung der Stellungnahme von Migros

2.1 Marketing

Empfehlung Nr. 1:

Der EDSB erlässt die Empfehlung, dass die Zweckumschreibung bezüglich der Warenkorbanalysen und Marketingauswertungen in den AGB präziser und für den Kunden transparenter formuliert wird: „Sie erlauben der Migros, Informationen über Ihre Einkäufe zu sammeln und zu Marketingzwecken auszuwerten. Gestützt auf Ihre Einkaufsdaten können Warenkorbanalysen durchgeführt werden, welche das Konsumverhalten sowie persönliche Kundenprofile widerspiegeln.“ (Ziff. 3 AGB).

Stellungnahme Migros:

Migros setzt die Empfehlung um und ändert ihre AGB wie folgt: *„Gestützt auf Ihre Einkaufsdaten können Warenkorbanalysen durchgeführt werden, welche das Konsumverhalten sowie persönliche Kundenprofile widerspiegeln können“ (Art. 3).*

Migros wird zusätzlich von sich aus in den AGB auf den Anmeldeformularen darauf hinweisen, dass die verbindliche Version der AGB jeweils auf www.m-cumulus.ch publiziert ist. Zusätzlich werden AGB-Änderungen jeweils im November allen CUMULUS-Teilnehmern im Rahmen des CUMULUS-Versandes mitgeteilt. Die AGB werden wie folgt ergänzt: *„Die aktuell gültigen Allgemeinen Geschäftsbedingungen sind jederzeit auf www.m-cumulus.ch abrufbar und gelten als von den Teilnehmern akzeptiert“ (Ziff. 13).*

Umsetzung: In Internet per Juni 2005; in Anmeldebroschüre per Juli 2005.

Reaktion EDSB:

Empfehlung wird umgesetzt. Auch wenn bei den AGB eine „kann“-Formulierung gewählt wurde, ist die Grundidee erhalten. Es sind keine weiteren Schritte nötig.

2.2 Werbung (von Migros)

Empfehlung Nr. 2:

Der EDSB erlässt die Empfehlung, dass entweder in der Anmeldebroschüre oder den AGB auf diesen Spezialversand hingewiesen wird, oder dass dieser Versand in Zukunft ganz unterlassen wird.

Stellungnahme Migros:

Migros sendet auf Wunsch der einzelnen Migros-Genossenschaften sog. „Aktuell“-Seiten mit lokalen Inhalten an M-CUMULUS Kunden. Auf die Zustellung der „Aktuell“-Seiten an Kunden, die keine Werbung wünschen, wird in Zukunft verzichtet.

Reaktion EDSB:

Die Empfehlung wird umgesetzt. Es sind keine weiteren Schritte nötig.

2.3 Werbung (von Partnern)

Anpassungs-/Verbesserungsvorschlag Nr. 1:

Sollte von der Migros in Zukunft in Betracht gezogen werden, im Rahmen von M-CUMULUS für Partnerunternehmen vermehrt gezielte Direktwerbung zu betreiben, so sind aus Sicht des EDSB dahingehende Präzisierungen in den AGB und in der Anmeldebroschüre vorzunehmen.

Stellungnahme Migros:

Der Absender von Partnerangeboten ist immer M-CUMULUS und den Kunden wird in der Anmeldung und den AGB offengelegt, dass sie Angebote erhalten. Dass sich diese Angebote auch auf Partnerunternehmen beziehen, stellt für Migros eine Selbstverständlichkeit dar. Deshalb erachtet Migros die Anpassung zwar als überflüssig, wird ihre AGB aber dennoch zugunsten der grösstmöglichen Transparenz wie folgt ergänzen: „Periodisch unterbreitet die Migros ihrer CUMULUS-Kundschaft spezielle CUMULUS-Angebote. Die Teilnehmer stimmen zu, über M-CUMULUS auch Angebote Dritter zu erhalten“ (Art. 12).

Umsetzung: In Internet per Juni 2005; in Anmeldebroschüre per Juli 2005.

Reaktion EDSB:

Der Vorschlag wird umgesetzt. Es sind keine weiteren Schritte nötig.

2.4 Auskunftsrecht

Anpassungs-/Verbesserungsvorschlag Nr. 2:

Trotz dieser positiven Bewertung des Auskunftsrechtes schlägt der EDSB vor, dass in den AGB explizit auf das Auskunftsrecht hingewiesen wird. Diese Anregung wurde bereits bei der Kontrolle vor Ort von den anwesenden Mitarbeitern des EDSB vorgebracht. Eine höhere Transparenz beim Auskunftsrecht rechtfertigt sich aus Sicht des EDSB gestützt auf die Tatsache, dass im Rahmen des Kundenbindungsprogramms M-CUMULUS mit sensiblen Personendaten umgegangen wird und hier deshalb die Kunden besser über ihr Auskunftsrecht aufzuklären sind.

Stellungnahme Migros:

Migros ist der Ansicht, dass aufgrund der Sensibilisierung gegenüber dem Datenschutz die Mehrheit der Kunden ihre Auskunftsrechte kennt. M-CUMULUS wies im Migros-Magazin zudem auf das Recht hin (Woche 6/2005). Ferner erfüllt Migros auf Anfrage der Kundschaft das Auskunftsrecht schnell, kostenlos und unkompliziert. Aus Sicht von Migros sollte zugunsten der Leserfreundlichkeit der AGB darauf verzichtet werden, die AGB mit Informationen zu ergänzen, welche bereits von Gesetz wegen geregelt sind.

Reaktion EDSB:

Der EDSB findet es notwendig, dass das Auskunftsrecht erwähnt wird und schlägt Migros nun vor, dass das Auskunftsrecht im Internet unter www.m-cumulus.ch/CUMULUS_DE/Content/UeberM-CUMULUS/Datenschutz/ (Rubrik Datenschutz) oder in den Frequently Asked Questions (FAQ) unter http://www.m-cumulus.ch/CUMULUS_DE/Content/UeberM-CUMULUS/FAQ erwähnt wird.

Migros ist damit einverstanden und wird wie vom EDSB vorgeschlagen das Auskunftsrecht unter der Rubrik Datenschutz und/oder FAQ erwähnen.

2.5 Datenlöschung auf Verlangen der Kunden

Anpassungs-/Verbesserungsvorschlag Nr. 3:

Ver mehrt noch als beim Auskunftsrecht drängt sich beim Löschungsrecht eine explizite Erwähnung in den AGB auf. Der EDSB regt an, dass dies vom MGB so umgesetzt wird.

Stellungnahme Migros:

Vgl. Ausführungen zu Anpassungs-/Verbesserungsvorschlag Nr. 2.

Reaktion EDSB:

Vgl. Ausführungen zu Anpassungs-/Verbesserungsvorschlag Nr. 2.

Anpassungs-/Verbesserungsvorschlag Nr. 4:

Gemäss dem Wortlaut geht der Kunde also davon aus, dass seine gesamten Konto-Daten gelöscht werden. Die Löschung bezieht sich aber tatsächlich nur auf die Stammdaten. Die Programmdateien werden anonymisiert und sind zu statistischen Zwecken weiterhin zugänglich. Dies sollte im Löschauftrag klargestellt werden.

Stellungnahme Migros:

Migros wird das Formular entsprechend korrigieren und das Wort „löschen“ im Zusammenhang mit dem Konto ersetzen. Die Information gegenüber den Kunden ist und war gemäss Migros klar und bleibt daher unverändert. Im Antragsformular, welches die Kundschaft an Migros zurücksendet, wird die Formulierung „...beauftrage ich MGB, bzw. M-CUMULUS, folgendes Konto zu löschen“ abgeändert. Sie lautet seit Ende Mai neu: „...beauftrage ich MGB, bzw. M-CUMULUS, die *Personalien* in folgendem Konto zu löschen“.

Umsetzung: per 1. Juni 2005 implementiert.

Reaktion EDSB:

Der Vorschlag wird umgesetzt. Es sind keine weiteren Schritte nötig.

2.6 Aufbewahrung und Löschung weiterer Daten**Anpassungs-/Verbesserungsvorschlag Nr. 5:**

Der EDSB fordert den MGB daher auf, dass in den AGB ein Vermerk aufgenommen wird, dass die im Rahmen des CUMULUS-Programms erhobenen Daten bis zu 3 Jahre aufbewahrt werden. Zusätzlich sollten für den Kunden relevante Aufbewahrungsfristen umschrieben werden und Fristen im Internet abrufbar aufgeführt werden.

Stellungnahme Migros:

Migros wird die Aufbewahrungsdauer persönlicher Daten im Internet unter www.m-cumulus.ch/CUMULUS_DE/Content/UeberM-CUMULUS/Datenschutz/ (Rubrik Datenschutz) publizieren:

Ihre Einkaufsdaten

Ihre Daten sind bei uns gut aufgehoben. Hier sehen Sie, wie lange wir welche Informationen aufbewahren:

Einkaufstotale werden 3 Kalenderjahre lang aufbewahrt. Die Zahlen zeigen uns, wie viel Sie wo ausgegeben haben (aber nicht, aus welchen Einzelpositionen sich ihr Einkauf zusammengesetzt).

Einkaufsdetaildaten werden 15 Monate lang aufbewahrt. Sie zeigen uns, was Sie wo eingekauft haben. Welche Produkte Sie eingekauft haben, wissen wir also nur 15 Monate lang.

Umsetzung: Im Sommer 2005

Reaktion EDSB:

Vorschlag wird umgesetzt. Keine weiteren Schritte nötig.

2.7 Sicherheit⁵

Anpassungs-/Verbesserungsvorschlag Nr. 6:

(...)

Stellungnahme Migros:

(...)

Reaktion EDSB:

(...)

2.8 Datentransfer ins Ausland

Anpassungs-/Verbesserungsvorschlag Nr. 7:

Darüber hinaus schlägt der EDSB jedoch noch vor, dass die Datenübermittlung mit Erwähnung des Destinationslandes in die AGB aufgenommen wird.

Stellungnahme Migros:

Eine Datenübermittlung ins Ausland ist bisher nur einmal vorgekommen und wurde dem EDSB gemeldet. Weiter Datenübermittlungen sind nicht vorgesehen. Deshalb ist auch ein Destinationsland einer zukünftigen Übermittlung nicht bekannt. Da ein Transfer aber nicht auszuschliessen ist, wird Migros die AGB wie folgt ergänzen: „Gestützt auf Ihre Kundendaten können Warenkorbanalysen durchgeführt werden, welche das Konsumverhalten sowie persönliche Kundenprofile widerspiegeln können. Dabei kann auch ein Datentransfer ins Ausland erfolgen. Es wird vertraglich sichergestellt, dass dabei keine über den konkreten Kundenauftrag hinausgehende Verwendung der Daten durch die bearbeitende Partnerfirma stattfindet und diese die Daten weder für sich verwendet, noch einem Dritten weitergibt“ (Art. 3).

Umsetzung: In Internet per Juni 2005; in Anmeldebroschüre per Juli 2005.

Reaktion EDSB:

Migros hat dem EDSB in seiner Stellungnahme darlegen können, weshalb die Nennung eines Destinationslandes in den AGB heute nicht möglich ist. Der EDSB begrüsst die Präzisierung der AGB bezüglich des Datentransfers ins Ausland. Falls der zeitlich limitierte Datentransfer nach Deutschland in ein Definitivum überführt werden oder in Zukunft ein Datentransfer in ein anderes Land erfolgen sollte, ist

⁵ Aufgrund überwiegender Interessen der Migros an der Vertraulichkeit dieser Angaben wurden die entsprechenden Passagen zur Datensicherheit (gesamte Ziff. 2.7) für die Publikation aus dem Bericht herausgenommen. Die Datenschutzkontrolle des EDSB hat gezeigt, dass die Sicherheitsmassnahmen **den Anforderungen des Datenschutzgesetzes entsprechen**.

das Destinationsland hingegen aus Sicht des EDSB in den AGB aufzuführen. Nach jetziger Sachlage kann jedoch von der Angabe des Destinationslandes abgesehen werden.

Der Vorschlag wird umgesetzt. Es sind keine weiteren Schritte nötig.

Bern, den 28. September 2005

**EIDGENÖSSISCHER
DATENSCHUTZBEAUFTRAGTER**

Der Beauftragte:

Hanspeter Thür