



A2014.03.24-0011

07.04.2014

Kundenbindungsprogramm Cumulus

Schlussbericht vom 7. April 2014

**der Kontrolle des
Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)
gemäss Art. 29 des Bundesgesetzes
über den Datenschutz (DSG)**



Inhaltsverzeichnis

1.	Ausgangslage	4
2.	Umfang der Kontrolle	5
3.	Chronologie der Kontrolle	5
4.	Grundlagen des Schlussberichtes	6
4.1.	Eingereichte Dokumentation / beantwortete Fragen im Vorfeld der Kontrolle	6
4.2.	Kontrolle vom 18. Juni 2013 vor Ort in Zürich	6
4.3.	Fact Sheet und beantwortete offene Fragen im Nachgang der Kontrolle	7
4.4.	Schema der Datenflüsse im Rahmen von Cumulus	7
5.	Anmeldung	7
5.1.	Untersuchte Datenflüsse	7
5.2.	Beurteilung aus Sicht des EDÖB	9
6.	Punktesammlung	11
6.1.	Untersuchte Datenflüsse	11
6.2.	Punktesammeln im Einzelnen	12
6.3.	Beurteilung aus Sicht des EDÖB	13
7.	Marketing	14
7.1.	Marketing im Einzelnen	14
7.2.	Beurteilung aus Sicht des EDÖB	15
8.	Werbung (von Migros)	16
8.1.	Untersuchte Datenflüsse	16
8.2.	Werbung im Einzelnen	17
8.3.	Beurteilung aus Sicht des EDÖB	18
9.	Werbung (von Partnern)	19
9.1.	Werbung von Partnern im Einzelnen	19
9.2.	Beurteilung aus Sicht des EDÖB	19
10.	Auskunftsrecht	20
10.1.	Untersuchter Datenfluss	20
10.2.	Auskunftsrecht im Einzelnen	20
10.3.	Beurteilung aus Sicht des EDÖB	21



11.	Datenauskünfte auf behördliche Anweisung	23
11.1.	Untersuchter Datenfluss	23
11.2.	Bekanntgabe von Kundendaten auf behördliche Anweisung im Einzelnen	23
11.3.	Beurteilung aus Sicht des EDÖB	24
12.	Datenlöschung auf Verlangen der Kunden	24
12.1.	Untersuchter Datenfluss	24
12.2.	Löschanträge im Einzelnen	24
12.3.	Beurteilung aus Sicht des EDÖB	25
13.	Aufbewahrung und Löschung weiterer Daten	26
13.1.	Untersuchter Datenfluss	26
13.2.	Aufbewahrung und Löschung weiterer Daten im Einzelnen	27
13.3.	Beurteilung aus Sicht des EDÖB	27
14.	Sicherheit	28
14.1.	Sicherheitsmassnahmen im Einzelnen	28
14.2.	Beurteilung aus Sicht des EDÖB	28
15.	Sensibilisierung und Schulung von Cumulus-Mitarbeitern	29
15.1.	Ergriffene Massnahmen und Beurteilung	29
16.	Ergebnisse	30
16.1.	Anmeldung	30
16.2.	Punktesammlung	32
16.3.	Marketing	32
16.4.	Werbung (von Migros)	32
16.5.	Werbung (von Partnern)	33
16.6.	Auskunftsrecht	34
16.7.	Datenauskünfte auf behördliche Anweisung	35
16.8.	Datenlöschung auf Verlangen der Kunden	36
16.9.	Aufbewahrung und Löschung weiterer Daten	36
16.10.	Sicherheit	37
17.	Schlussfolgerungen	38
17.1.	Bezüglich der Kontrolle des Kundenbindungsprogramms Cumulus	38
17.2.	Verfahren und weiteres Vorgehen	38



1. Ausgangslage

Migros bietet seit dem 1. November 1997 ihren Kunden das Bonusprogramm Cumulus an. Der Benutzerkreis ist in dieser Zeit stetig gewachsen. Heute nutzen rund 2,7 Mio. Haushalte in der Schweiz aktiv eine Cumulus-Karte.

Im Jahre 2005 hat der EDÖB eine Datenschutzkontrolle gemäss Art. 29 des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1) beim Migros durchgeführt. Die Ergebnisse wurden im Schlussbericht vom 23. Mai 2005 festgehalten. Zusammen mit diesem Bericht wurden vom EDÖB verschiedene Anpassungs- resp. Verbesserungsvorschläge oder Empfehlungen im Sinne des Art. 29 Abs. 3 DSG formuliert. Nach beinahe 10 Jahren erachtet es der EDÖB als angebracht, eine Nachkontrolle bei Migros durchzuführen. Ziel dieser Kontrolle ist einerseits die Überprüfung der Umsetzungen dieser Anpassungsvorschläge oder Empfehlungen und andererseits sollen die wesentlichen Neuerungen oder Änderungen im Zusammenhang mit dem Cumulus-Programm aus datenschutzrechtlicher Sicht beurteilt und festgehalten werden.

In den vergangenen Jahren hat es in den Kernprozessen von Cumulus keine wesentlichen Veränderungen gegeben: Der Cumulus-Teilnehmer kauft ein und sammelt dabei Cumulus-Punkte, wenn er seine Kundenkarte an der Kasse vorzeigt. Neuerungen wurden z.B. mit dem Online-Club für Familien „Famigros“ eingeführt, welcher sich an Mütter und Väter mit Kinder richtet. Zudem wurde die Spendemöglichkeit lanciert, wo ein Kunde seine gesammelten Punkte einem anderen Kunden oder einer Organisation übertragen kann.

Seit 2002 unterstellt sich Cumulus selbstverpflichtend dem Datenschutzgütesiegel „Good Priv@cy“. Cumulus verfügt zudem über ein Datenschutz-Manual, welches anfangs 2012 überarbeitet wurde. Darin werden die zentralen Datenschutz-Grundsätze für Cumulus definiert und kommuniziert.



2. Umfang der Kontrolle

Im Rahmen der Nachkontrolle des EDÖB wurden die Datenflüsse im Zusammenhang mit dem Kundenbindungsprogramm Cumulus kontrolliert.

Die Kontrolle fokussierte sich auf die Umsetzung der Änderungs- resp. Verbesserungsvorschläge oder Empfehlungen des Schlussberichtes vom 23. Mai 2005 sowie die Beurteilung und Festhaltung der wesentlichen Neuerungen oder Änderungen im Zusammenhang mit dem Cumulus-Programm.

3. Chronologie der Kontrolle

April 2013	Beschluss des EDÖB zur Durchführung einer Nachkontrolle beim Migros-Genossenschafts-Bund (im Folgenden MGB) im Rahmen des Kundenbindungsprogramms Cumulus.
16. Mai 2013	Ankündigung der Kontrolle beim MGB mit der Bitte um Dokumentation über das Kundenbindungsprogramm und Beantwortung von Zusatzfragen.
10. Juni 2013	Eingang der Unterlagen und Dokumente von Migros (eingereicht durch Cumulus Marketing Services und MGB Rechtsabteilung).
18. Juni 2013	Durchführung der Datenschutzkontrolle vor Ort am Hauptsitz des MGB in Zürich.
25. Juli 2013	Zusendung eines Fact Sheets der Datenschutzkontrolle vom 18. Juni 2013 an die Rechtsabteilung MGB zur Konsultation und Bitte um materielle Berichtigung.
21. August 2013	Eingang der Antworten auf die noch offenen Fragen des EDÖB mit materieller Berichtigung des Fact Sheets.
7. April 2014	Verabschiedung des Schlussberichtes durch den EDÖB.



4. Grundlagen des Schlussberichtes

4.1. Eingereichte Dokumentation / beantwortete Fragen im Vorfeld der Kontrolle

Der vorliegende Bericht stützt sich auf den Schlussbericht vom 23. Mai 2005, die vom MGB eingereichte Dokumentation im Vorfeld der Nachkontrolle sowie auf die in diesem Zusammenhang ebenfalls beantworteten Fragen des EDÖB zu den Datenbearbeitungen und Datenflüssen. Insofern widerspiegelt der Schlussbericht eine *Bestandesaufnahme* der Datenbearbeitung, wie sie dem EDÖB im Juni 2013 anhand der vorhandenen resp. eingereichten Dokumentation sowie anhand der Sitzung vor Ort bekannt waren.

4.2. Kontrolle vom 18. Juni 2013 vor Ort in Zürich

Am 18. Juni 2013 hielt der EDÖB in den Räumlichkeiten am Hauptsitz des MGB in Zürich eine Sitzung mit den in das Cumulus-Programm involvierten Akteure ab. Dieser Augenschein vor Ort bildet ebenfalls eine wichtige Grundlage für den vorliegenden Kontrollbericht.

Anwesende Personen

Von Seiten der Migros waren die Projektleiterin Cumulus und Datenschutzverantwortliche Cumulus, der stv. Leiter Direktion Recht MGB, der Leiter Cumulus, der Leiter Customer Intelligence, der Leiter Datawarehouse Solution / IT-Cumulus, der Fachbereichsleiter BI/CRM/Cumulus / IT-Cumulus sowie die Leiterin Cumulus-Infoline anwesend.

Der EDÖB war durch einen Juristen und einen Informatiker vor Ort vertreten.

Besichtigte Unterlagen/Präsentationen

In chronologischer Abfolge:

- Grundlagen in das Cumulus-Programm
- Änderungen Cumulus im Vergleich zum Schlussbericht von 2005
- Präsentation der Marketingauswertung im Rahmen von Cumulus
- Handhabung des Auskunftsbegehrens



4.3. Fact Sheet und beantwortete offene Fragen im Nachgang der Kontrolle

Migros hat vom EDÖB eine Zusammenstellung der wesentlichen Grundlagen des Cumulus-Programms erhalten, wie es die Mitarbeiter des EDÖB gestützt auf die erhaltenen Unterlagen und gestützt auf die Sitzung vor Ort verstanden haben (sog. Fact Sheet).

Dieses Fact Sheet wurde Cumulus Marketing Services und der Rechtsabteilung des MGB zur Konsultation unterbreitet, mit Bitte um materielle Berichtigung. Das bereinigte Fact Sheet sowie die Antworten auf die Rückfragen stellen ebenfalls eine wichtige Grundlage für den vorliegenden Schlussbericht dar.

4.4. Schema der Datenflüsse im Rahmen von Cumulus

Da bezüglich den Datenflüssen bei Cumulus keine Änderungen festgestellt werden konnten, kann hier auf die Schemata im Schlussbericht vom 23. Mai 2005 verwiesen werden.

5. Anmeldung

5.1. Untersuchte Datenflüsse

Die Anmeldung zum Cumulus-Programm kann zum einen mit dem klassischen Anmeldetalon in der Anmeldebroschüre erfolgen, welche in jeder Migros-Filiale aufliegt. Darin enthalten sind detaillierte Angaben zu Cumulus, eine Auflistung aller Programmpartner, bei denen Punkte gesammelt resp. wieder eingelöst werden können, eine Cumulus-Karte, 4 Kleber mit der Cumulus-Nummer, Angaben zur Cumulus-Infoline und die allgemeinen Geschäftsbedingungen (im Folgenden AGB). Der Kunde füllt den Talon mit seinen persönlichen Daten aus und sendet diesen an die Migros. Der Talon wird intern in der Migros an das externe Call Center (sog. „Cumulus-Infoline“; Betreiberin ist die avocis TELAG [im Folgenden TELAG]) geschickt, welches die Daten in die Cumulus-Datenbank überträgt.

Zweitens können Kunden gegenüber der Prozessbeschreibung von 2005 heute auch über ein Online-Formular auf der Homepage von Cumulus Mitglieder werden (Link: <https://www.migros.ch/cumulus/de/ueber-cumulus/cumulus-mitglied-werden.html>). Migros



informiert auf dieser Homepage, wo die Kunden Cumulus-Punkte sammeln und einlösen können. Die AGB sind per Link einsehbar und müssen bei der Anmeldung vom Kunden aktiv bestätigt werden (siehe unten). Zusätzlich informiert Migros am Ort dieser AGB-Bestätigung nochmals, dass Migros die Daten für weitere Zwecke (Marketing, Auswertungen, Statistik) verwenden darf. Diese Information entspricht im Wesentlichen der gedruckten Version auf dem Anmeldetalon (siehe folgend).

Ich möchte auf Werbung/Angebote verzichten.

Ich akzeptiere die [Allgemeinen Geschäftsbedingungen](#) *¹

Ich möchte weltweit, auch ausserhalb der Migros, Cumulus-Punkte sammeln - mit der gratis Cumulus-MasterCard (keine Jahresgebühr, auch in den Folgejahren). Bitte senden Sie mir Informationen dazu.

*1) Mit Ihrer Anmeldung gestatten Sie der Migros ausdrücklich, über die Cumulus-Karte erhaltene Daten für weitere Zwecke (Marketing, Auswertungen, Statistik) zu verwenden. Alle Personendaten werden streng vertraulich behandelt und nicht ausserhalb der Migros-Gemeinschaft (alle Migros-Fillialen, -Fachmärkte, -Dienstleistungs- und -Produktionsbetriebe) weitergegeben. Cumulus ist eine Haushaltskarte (private Haushalte). Jede Person im Haushalt kann mit demselben Cumulus-Strichcode auf das Cumulus-Konto Punkte sammeln.

Zusätzliche Informationen findet der interessierte Kunde auf der Homepage von Cumulus. Dort befindet sich auch eine Rubrik „Datenschutz“, wo die Migros u.a. über das Auskunfts-, das Löschungsrecht und die Aufbewahrungszeiten der Daten informiert und Formulare zur Verfügung stellt.

Obligatorische Angaben sowohl bei der Anmeldung per Anmeldetalon als auch mit dem Online-Formular sind: Anrede, Vorname, Nachname, Strasse, PLZ und Ort, Land und Geburtsdatum. Zusätzlich wird bei der Online-Anmeldung eine E-Mail-Adresse verlangt, da hier ein Anmelde-Bestätigungsmail auf die angegebene Adresse erfolgt. Grundsätzlich sind die Angaben zur Haushaltsgrösse und das Geburtsdatum auch auf dem Anmeldetalon als obligatorische Angaben deklariert, eine Anmeldung wird jedoch in der Praxis auch ohne diese Daten akzeptiert.

In Ziffer 3 der AGB informiert Migros über den Zweck der Datensammlung von Cumulus. Darin wird erwähnt, dass Migros Informationen über die Einkäufe sammeln und für Marketingzwecke auswerten darf. Weiter heisst es, dass *„gestützt auf die Einkaufsdaten bei Unternehmen der*



M-Gruppe Warenkorbanalysen durchgeführt werden können, die das Konsumverhalten sowie persönliche Personenprofile der betroffenen Person widerspiegeln können“.

Kunden haben bei beiden Anmeldeformen die Möglichkeiten, vom Angebot auf Direktwerbung zu verzichten (Opting-out). Dieser Verzicht kann gemäss Migros auch noch nachträglich geltend gemacht werden (z.B. über die Cumulus-Infoline). Darüber hinaus können Kunden mit der Anmeldung gleichzeitig Informationen über die Cumulus-MasterCard bestellen.

Bei sogenannten Aktionen mit „Cumulus-Vorteilen“ kann der Cumulus-Kunde von weiteren zeitlich begrenzten Aktionen profitieren, beispielsweise einen Velohelm mit 25% Rabatt.

Anmeldungen, wo Kunden Änderungen an den AGB vorgenommen haben, werden nicht akzeptiert. Die Kunden werden von der Cumulus-Infoline schriftlich in Kenntnis gesetzt, dass sie nicht am Cumulus-Programm teilnehmen können.

Am 16. März 2012 lancierte die Migros den Klub für Familien „Famigros“ (www.famigros.ch). Der bisherige „Babyclub“ wurde Ende April 2012 aufgehoben. „Famigros“ richtet sich an Mütter und Väter mit Kindern, bzw. ab Schwangerschaft bis zum 25. Lebensjahr des Nachwuchses; daneben können die Familien ihr Haustier bei der Anmeldung angeben. Eine Anmeldung zu „Famigros“ ist nur online möglich und dies nur für bestehende Cumulus-Kunden. Folgende Angaben können bei der Anmeldung gemacht werden: Angaben zu den Kindern (Geschlecht, Name, Geburtsdatum), Angaben zur Schwangerschaft (Voraussichtlicher Geburtstermin) und Angaben zu den Haustieren (Art/Gattung, Name, Geburtsdatum). Der Klub bietet den Kunden u.a. gewisse Vergünstigungen (z.B. Eintritt in den Europa-Park) und diverse praktische Informationen auf der Homepage von „Famigros“.

5.2. Beurteilung aus Sicht des EDÖB

Die Angaben auf der Anmeldung sind Personendaten im Sinne des Datenschutzgesetzes, für deren Bearbeitung ein Rechtfertigungsgrund (Art. 12 und 13 DSG) benötigt wird. Als Rechtfertigungsgrund der Datenbearbeitung kommt im vorliegenden Fall die Einwilligung der betroffenen Personen in Frage. Eine rechtlich gültige Einwilligung setzt nach Art. 4 Abs. 5 Satz 1 voraus, dass a) eine angemessene Information bezüglich der Datenbearbeitung vorliegt, in die eingewilligt werden soll; b) eine Willenserklärung vorliegt, aus welcher die Zustimmung zu



dieser Datenbearbeitung entnommen werden kann und c) die Willenserklärung freiwillig erfolgt. Die Kunden geben mit der Anmeldung zum Kundenbindungsprogramm Cumulus 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. Bei gewissen Produkten im Rahmen von Aktionen mit „Cumulus-Vorteil“ ist der Kunde auf den Besitz der Cumulus-Karte angewiesen, um von dem Preisvorteil zu profitieren. Dieser Umstand kann unter dem Aspekt der Freiwilligkeit der Einwilligung zur Datenbearbeitung resp. Teilnahme am Cumulus-Programm problematisch sein. Die Aktionen sind zeitlich und von der Produktmenge und -wahl derart zu beschränken resp. zu wählen, dass eine echtes Alternativverhalten aus der Sicht der Kundschaft gewährleistet ist, das heisst, dass die Kunden, welche nicht im Besitz einer Cumulus-Karte sind, vergleichbare Angebote ohne Cumulus-Karte beziehen können. Aus heutiger Sicht ist dies gewährleistet. Sollen die Aktionen mit „Cumulus-Vorteil“ in Zukunft ausgedehnt werden, kann u.U. nicht mehr von einer freiwilligen Einwilligung und damit von einer rechtsgültigen Einwilligung im Sinne von Art. 4 Abs. 5 Satz 1 DSGVO gesprochen werden.

Die Bearbeitung von Personendaten muss nach Treu und Glauben erfolgen (Art. 4 Abs. 2 DSGVO). Daten sollen nicht in einer Art erhoben werden, mit der die betroffene Person aus den Umständen heraus nicht rechnen musste und mit der sie nicht einverstanden gewesen wäre. Die Datenbearbeitung muss für die betroffenen Personen transparent erfolgen. Aufgrund des gesamten Prozederes ist den Cumulus-Antragsstellern klar, dass es sich um eine Kundenkarte handelt, und dass Migros grundsätzlich die Angaben von Cumulus für Werbung nutzen kann. Explizit informiert Migros einerseits direkt bei der Anmeldung und andererseits in Ziffer 3 der AGB über die Datenbearbeitung im Zusammenhang mit dem Cumulus-Programm. Hier wird dem Kunden mitgeteilt, dass „die Einkaufsdaten bei Unternehmen der M-Gruppe gesammelt und eine Warenkorbanalyse vorgenommen wird. Daraus werden Angaben zum Konsumverhalten und Personenprofile ermittelt“. Sowohl auf der Anmeldebroschüre wie auch auf der Website 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 transparent (Art. 4 Abs. 2 DSGVO). Es wird 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.



Bezüglich der Stammdaten erfolgt die Datenerhebung in inhaltlicher Sicht verhältnismässig (Art. 4 Abs. 2 DSG).

Nach Art. 12 Abs. 2 lit. b DSG kann eine betroffene Person die Bearbeitung bzw. die weitere Bearbeitung ihrer Personendaten untersagen. Cumulus-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. Wird das entsprechende Feld nicht angekreuzt, willigt der Kunde implizit in eine weitere Datennutzung seiner Adressdaten ein (Art. 13 Abs. 1 DSG; vgl. dazu aber Ziff. 8.3).

Im Unterschied zur klassischen Anmeldung mittels Anmeldebroschüre finden sich auf der Homepage von Cumulus wesentliche datenschutzrechtliche Informationen zum Auskunfts- und Löschungsrecht und zu den Aufbewahrungszeiten der Daten in der Rubrik „Datenschutz“. Diese datenschutzrechtlichen Informationen zu den tragenden Datenschutzrechte sind auch in der Anmeldebroschüre mitzuteilen. Im Sinne des Transparenzgebots (Art. 4 Abs. 2 DSG) schlagen wir deshalb vor, auf der Anmeldebroschüre direkt bei den AGB ein Hinweis auf weitere Informationen und dem Formular über die Auskunftserteilung auf der Homepage abzudrucken (vgl. dazu auch Ziff. 10.2.,10.3 und 12.3).

6. Punktesammlung

6.1. Untersuchte Datenflüsse

Wie bis anhin, kann ein Kunde, der in der Migros oder einem Sammelpartner einkauft, 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. Die gesammelten Einkaufsdaten von den Kassen werden während der Nacht jeweils an den MGB-Server transferiert. Alle zwei Monate erhält ein Kunde eine Abrechnung per Post, auf der sein Punktestand und die gutgeschriebenen Cumulus-Punkte ersichtlich sind.

6.2. Punktesammeln im Einzelnen

Kunden, die am Cumulus-Programm teilnehmen, können bei jedem Einkauf mit Vorweisen der Cumulus-Karte 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. Anfangs 2013 führte Migros die Bonus-Coupons ein: Kunden erhalten ab Fr. 100.—an der Kasse einen 2-fach-Bonus-Coupon, resp. einen 5-fach-Bonus-Coupon für Einkäufe ab Fr. 500.--. Dieser Bonus-Coupon ist bis zum Ende des Folgemonats in den Migros-Supermärkten oder in den Fachmärkten SportXX, MElectronics, Micasa und Do it + Garten einlösbar. Die so gesammelten Bonus-Cumulus-Punkte erhalten die Kunden mit allen ihren anderen Punkten wie gewohnt alle 2 Monate in Form von blauen Cumulus-Bons ausbezahlt.

Cumulus-Punkte sammeln und einlösen kann man in folgenden Märkten: Migros, Migros-Restaurant, micasa, Le Shop.ch, SportXX, exlibris, melectronics, OutdoorSportXX, Do it + Garten, OBI, Migrol, migrolino, Migros Ferien und Migros Partner. Nur sammeln in Migrosbank, Mobility, Depot, travel.ch, m-way und Eurocentres. Seit 2005 sind folgende Sammelpartner dazukommen: Depot, m-way, Eurocentres, Migros Ferien, Mobility und Cumulus-Mastercard (Cembra Money Bank).

Im November 2012 wurde mit Cumulus-Extra eine weitere Einlöse-Art eingeführt. Die Kunden können dabei die blauen Cumulus-Bons auf der Cumulus-Homepage in Gutscheine von ausgesuchten Partnern eintauschen und so den Wert ihrer Bons vervielfachen.

Statt die Punkte einzulösen können die Cumulus-Kunden ihre Punkte seit kurzem einer gemeinnützigen Organisation oder einem beliebigen anderen Cumulus-Teilnehmer spenden. Der Spendenauftrag kann online ausgelöst bzw. geändert oder gelöscht werden. Auf der Homepage von Cumulus werden verschiedene Organisationen als Spendenempfänger empfohlen. Die Spendenempfänger erhalten jeweils die Vor- und Nachnamen ihrer Spender.



Die vom „Famigros“-Kunden hinterlegten Daten, welche bei der Anmeldung von den Kunden angegeben wurden, werden ausschliesslich für „Famigros“- oder Cumulus-Auswertungen verwendet. Eine Bekanntgabe an Dritte ausserhalb der M-Gruppe findet nicht statt.

6.3. Beurteilung aus Sicht des EDÖB

Die Bearbeitung von Personendaten hat sich am Grundsatz der Verhältnismässigkeit auszurichten (Art. 4 Abs. 2 DSG). Verhältnismässigkeit bedeutet, dass ein Datenbearbeiter nur diejenigen Daten bearbeiten darf, die zur Erreichung eines bestimmten Zwecks objektiv geeignet und tatsächlich erforderlich sind, und dass die Nachteile, die mit der Bearbeitung verbunden sind, in einem angemessenen Verhältnis zu den Vorteilen stehen müssen. Die Kunden können Punkte nur sammeln, wenn sie ihre Cumulus-Karten an der Kasse vorweisen. Insofern kann die betroffene Person selber bestimmen, wann sie mit ihrem Einkauf Punkte (und damit personenbezogene Daten) geniessen will und wann nicht. [REDACTED]

[REDACTED] Insofern kann das Kaufverhalten einer Person nicht heimlich oder ohne ihr Wissen festgehalten werden (Datenbearbeitung nach Treu und Glauben, Art. 4 Abs. 2 DSG und mit Einwilligung, Art. 13 DSG).

Der Datenfluss zwischen Migros und den Sammelpartnern erfolgt per gesicherter Übermittlung der Cumulus-Nummer via HTTPS (Webservice) mit einem SSL-Zertifikat geschützt. Weitere persönliche Daten (wie Name und Personalien) werden im Rahmen der Punktesammlung nicht bearbeitet. Bezüglich der Kombination der Cumulus-Karte mit einer Mastercard-Option ist anzumerken, dass Migros keine Kredit- oder Debitkartennummer speichert. Eine Verbindung von Cumulus-Nummer zur Zahlkarten-Nummer gibt es aus Sicherheitsgründen nicht. Bei jedem Einkauf ist bekannt, ob bar oder mit welcher Art („Brand“) von Zahlkarte der Hauptbetrag erfolgt ist. In diesem Sinne erfolgt die Datenbearbeitung verhältnismässig (Art. 4 Abs. 2 DSG).

Für den Versand der zweimonatlichen Cumulus-Schreiben an die Kunden liefert die IT-Cumulus die notwendigen Daten an die Druckerei. Nach dem Erstellen und Versand der Mailings werden die Daten bei der Druckerei gelöscht. In diesem Sinne erfolgt die Datenbearbeitung verhältnismässig (Art. 4 Abs. 2 DSG).



Bezüglich den Spenden werden auf der Cumulus-Datenbank die Spender bzw. die Spendenempfänger vermerkt. Die Daten werden ausschliesslich zur Sicherstellung des Spendenbetrages verwendet und nicht weiter verwendet. Auch hier erfolgt die Datenbearbeitung verhältnismässig (Art. 4 Abs. 2 DSG). Spender werde auf der Homepage unter der Rubrik „Fragen & Antworten“ darüber informiert, dass die Spendenempfänger Vor- und Nachname des Spenders erhalten. Insofern ist diese Datenbearbeitung transparent (Art. 4 Abs. 2 DSG).

7. Marketing

7.1. Marketing im Einzelnen

Die detaillierten Einkaufsdaten von Cumulus-Kunden werden in der Cumulus-Datenbank festgehalten. In der Abteilung Marketing Analysen erfolgt die Auswertung der Daten zu Marketing- sowie statistischen Zwecken. Die häufigsten Analysen werden hier auf aggregierten Ebenen vorgenommen, z.B. Anzahl Kunden in der Filiale XY letzte Woche, durchschnittliche Einkaufshäufigkeit in der Kategorie „BeautySelfcareWorld“ im vergangenen Jahr und dergleichen. Des weiteren werden Analysen zum Zwecke der Kundensegmentierungen vorgenommen.

[REDACTED]

Markterhebungen können im TCRM (= Total Customer Relationship Management) bis zum Kauf eines einzigen Produktes vorgenommen werden. Wie bereits in Bericht von 2005 festgehalten, würde der Vollzugriff auf die Cumulus-Daten es 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. 11) muss durch die Cumulus Marketing Services freigegeben werden. In dieser internen Weisung ist auch festgehalten, dass keine Personendaten direkt an irgendwelche interne oder externe Interessierte (d.h. an Dritte) oder Auftraggeber (d.h. Trägerunternehmen oder Partnerunternehmen, welche Adressanträge stellen) geliefert werden. Die Datenbankzugriffe werden zudem protokolliert, jedoch finden davon keine Auswertungen statt. In den regelmässigen Schulungen und im Rahmen von Audits wird immer wieder auf das Verbot der Einzel-Auswertungen aufmerksam gemacht.

Entsprechende Auswertungsanträge im Hinblick auf Direct Marketing Aktionen laufen immer über die Cumulus Marketing Services.

7.2. Beurteilung aus Sicht des EDÖB

Gemäss Art. 3 lit. d DSG stellt eine Zusammenstellung einer grösseren Zahl von Daten über die Persönlichkeitsstruktur, die beruflichen Fähigkeiten oder auch die die ausserberuflichen Beziehungen und Tätigkeiten, die ein Gesamtbild oder ein wesentliches Teilbild der betroffenen Person ergeben, ein Persönlichkeitsprofil dar. Mit der Nutzung der Cumulus-Karte speichert Migros sämtliche Einkäufe der bei ihr registrierten Kunden (falls die Karte an der Kasse vorgezeigt wird) und kann sich so ein Bild von den Konsumgewohnheiten der Personen machen, was einem Persönlichkeitsprofil im Sinne von Art. 3 lit. d DSG entspricht. Ob die Kundenkarte von mehreren Personen zugleich benutzt wird, spielt keine Rolle, da der Grossverteiler die Angaben einer bestimmten Person, d.h. dem registrierten Kunden, zuordnen wird, mit dessen Einwilligung allenfalls auch weitere Personen die Kundenkarte benutzen.

Mit der Beschaffung von besonders schützenswerten Personendaten oder Persönlichkeitsprofile ist eine erweiterte Informationspflicht des Dateninhabers verbunden. Diese ist in Art. 14 DSG geregelt. Gemäss Abs. 2 muss der Inhaber der Datensammlung der betroffenen Person – in der Regel ausdrücklich – alle Informationen zukommen lassen, die für eine Bearbeitung nach dem Grundsatz von Treu und Glauben und der Verhältnismässigkeit



erforderlich sind. Es sind dies mindestens die Informationen gemäss den Buchstaben a bis c, das heisst die Identität des Inhabers der Datensammlung, den Zweck des Bearbeitens und die Kategorien allfälliger Datenempfänger wie in Ziff. 5.2 festgehalten, erfolgt diese Information korrekt.

Wie im Bericht des EDÖB von 2005 festgehalten, kann im TCRM in Verbindung mit dem Cumulus-Dialogsystem („CuDi“), wo alle Stamm- und Programmdateien abrufbar sind, Erhebungen über das Kaufverhalten der Cumulus-Kundschaft bis zum Kauf eines einzigen Produktes vorgenommen werden. Gestützt auf die Erhebung von Warenkörben steht der Marketing Abteilung eine enorme Auswahl an Kriterien zur Markt- und Kundenerforschung offen. Aufgrund dieser Feststellung hat der EDÖB 2005 die Empfehlung (Empfehlung Nr. 1) erlassen, dass die Zweckumschreibung bezüglich der Warenkorbanalyse und Marketingauswertungen in den AGB präziser und für den Kunden transparenter formuliert werden soll. In Ziffer 3 der aktuellen AGB informiert Migros, dass „Gestützt auf Ihre Einkaufsdaten bei Unternehmen der M-Gruppe können Warenkorbanalysen durchgeführt werden, die das Konsumverhalten sowie persönliche Personenprofile widerspiegeln können.“ In Ziff. 10 AGB wird informiert, dass die aktuell gültigen AGB jederzeit unter www.migros.ch/cumulus abrufbar sind. Damit wurde die Empfehlung des EDÖB aus dem Schlussbericht von 2005 vollumfänglich umgesetzt.

8. Werbung (von Migros)

8.1. Untersuchte Datenflüsse

Die Abteilung Customer Web Analyse (CWI) kann im Auftrag von Cumulus Marketing Services die Daten von Cumulus-Kunden analysieren und gestützt darauf kundenspezifische Werbung (Direct Marketing Aktionen) lancieren. Die Auswahlkriterien der Marketinganalysen für diese 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) gedruckt und die Werbung direkt an die einzelnen Haushalte verschickt.



8.3. Beurteilung aus Sicht des EDÖB

Bezüglich der Voraussetzungen für eine rechtsgültige Einwilligung kann auf Ziff. 5.2. verwiesen werden. Eine Einwilligung ist vor der fraglichen Datenbearbeitung jederzeit und frei widerruflich (Art. 27 Abs. 2 Schweizerisches Zivilgesetzbuch [ZGB]; SR 210). 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. Migros akzeptiert jedoch auch eine Verzichtserklärung zu einem späteren Zeitpunkt; eine Information über die nachträgliche Verzichtsmöglichkeit fehlt jedoch. Im Sinne der vollständigen Transparenz über das Recht der jederzeitigen freien Widerrufbarkeit der Einwilligung ist hier eine Ergänzung in den AGB anzubringen.

Die Einkaufsdaten der Kunden werden auch bei einer Verzichtserklärung weiterhin für Marketingzwecke analysiert. Ein Verzicht auf die Warenkorbanalyse ist nur in Verbindung mit dem Austritt aus dem Cumulus-Programm möglich. Dass in Zukunft eine kanalspezifische An- resp. Abmeldung für Werbekontakte vorgesehen wird, ist zu begrüssen.

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. Der EDÖB hat deshalb im Schlussbericht vom 23. Mai 2005 die Empfehlung erlassen (Empfehlung Nr. 2), dass bezüglich eines Spezialversandes in der Anmeldebroschüre oder den AGB hingewiesen wird oder dass dieser Versand in Zukunft ganz unterlassen wird. Da die „Aktuell“-Beilage weggefallen ist und kein weiterer Spezialversand festgestellt werden konnte, wurde der Empfehlung Nr. 2 vollumfänglich entsprochen.

Personendaten dürfen nur für den Zweck bearbeitet werden, welcher bei der Beschaffung angegeben worden ist oder aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSG). Der Verwendungszweck der Daten muss bereits bei der Datenbeschaffung ersichtlich sein oder sonst feststehen. Der EDÖB begrüsst die Tatsache sehr, dass Adressdaten nie an Partnerunternehmen direkt herausgegeben werden und damit das Risiko einer Zweckentfremdung (vgl. Art. 4 Abs. 3 DSG) möglichst gering gehalten wird.



9. Werbung (von Partnern)

9.1. Werbung von Partnern im Einzelnen

Gegenüber der Sachverhaltsfeststellung von 2005 hat sich in den Prozessen nichts verändert. Die Generali-Versicherung ist als Partnerunternehmen ausgeschieden, neue Partner sind keine hinzugekommen.

9.2. Beurteilung aus Sicht des EDÖB

Den Partnerunternehmen werden die sondierten Adressdaten der Cumulus-Kundschaft nie direkt ausgehändigt. Insofern erscheint 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 DSG) gewährleistet. Zusätzlich wird vertraglich klargestellt, dass 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 DSG) und tritt der Gefahr einer Zweckentfremdung (vgl. Art. 4 Abs. 3 DSG) durch Migros-externe Partnerunternehmen entgegen.

Im Schlussbericht vom 23. Mai 2005 unter Ziff. 5.5.3 wurde festgehalten, dass für die Cumulus-Kundschaft die Möglichkeit der indirekten Datennutzung durch Partnerunternehmen für gezielte Direktwerbung wenig ersichtlich ist. 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 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 EDÖB eine Präzisierung in der Anmeldebroschüre oder den beigelegten AGB auf. Zugunsten einer grösstmöglichen Transparenz sollen die AGB wie folgt ergänzt werden:



„Periodisch unterbreitet die Migros ihrer Cumulus-Kundschaft spezielle Cumulus-Angebote. Die Teilnehmer stimmen zu, über Cumulus auch Angebote Dritter zu erhalten.“ Diese Formulierung fehlt in den aktuellen AGB. Wir schlagen deshalb eine Ergänzung vor.

10. Auskunftsrecht

10.1. Untersucher Datenfluss

Das Auskunftsrecht (Art. 8 DSGVO) kann ein Kunde entweder über das Call Center oder über das Formular auf der Cumulus-Homepage geltend machen. Ferner hat er die Möglichkeit, seinen Punktestand und sein Kundenkonto per Internet abzufragen.

10.2. Auskunftsrecht im Einzelnen

Die TELAG mit Sitz in Zürich betreibt die Cumulus-Infoline. Sie beschäftigt in ihren Räumlichkeiten 25-30 Personen für die Cumulus-Infoline. Das Auskunftsrecht wird auf der Webseite von Cumulus unter der Rubrik Datenschutz ausdrücklich erwähnt. Dort findet sich auch ein Formular, wo die betroffene Person schriftlich Auskunft über die gespeicherten Daten von Cumulus verlangen kann. Die auskunftssuchende Person kann wählen, ob sie alle Informationen über die gespeicherten Personalien und weitere Cumulus-Programmrelevante Informationen und/oder auch alle Einkaufsdaten (mit Kassenzetteltotalen pro Einkauf inkl. Datum inkl. einzelne eingekaufte Produkte) haben will. Auf der (gedruckten) Anmeldebroschüre und in den AGB im Speziellen findet sich kein Hinweis auf das Auskunftsrecht.

Von den Kunden wird verlangt, dass sie sich mit der Kopie eines amtlichen Ausweises identifizieren. Alle beantragten und eingegangenen Auskunftsbegehren werden im „CuDi“ vermerkt. Bis heute sind Auskunftsgesuche (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. Für die mündlichen Auskunftsbegehren bestehen schriftliche Anweisungen (DMS-Handbuch). Bei sehr komplexen oder heiklen Anfragen wird der Rechtsdienst MGB konsultiert.



Die Cumulus-Kundschaft hat auch die Möglichkeit, per Online-Account im Internet Einblick in ihre Cumulus-Daten zu erhalten. Hier können die Personalien, der kumulative Einkaufsbetrag und die kumulative Punktezahl der laufenden Periode sowie ein Abbild der Kontoauszüge der Abrechnungsperioden (PDF) über die letzten zwei Jahre eingesehen werden. Der Kunde kann sich daneben den gesamten Warenkorb der vergangenen 2 Jahre anzeigen lassen. 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).

Auf der Auskunftserteilung werden dem Kunden ein ausführlicher Auszug aus der Datenbank mit den Kundenstammdaten und auf Verlangen die Einkaufsdaten mit Kassenzetteltotalen pro Einkauf mit Datum und alle einzelne eingekaufte Produkte mitgeteilt. Über die Kundensegmentierung aufgrund der Analyse seiner Einkaufsdaten resp. Einkaufsverhalten erhält der Kunde keine Informationen.



10.3. Beurteilung aus Sicht des EDÖB

Gemäss Art. 8 DSG kann jede Person vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über die bearbeitet werden. Der Inhaber der Datensammlung muss der betroffenen Person mitteilen:

- Alle über sie in der Datensammlung vorhandenen Daten einschliesslich der verfügbaren Angaben über die Herkunft der Daten;
- Den Zweck und gegebenenfalls die Rechtsgrundlagen des Bearbeitens sowie die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger.

Betroffene Personen können gemäss Art. 15 DSG eine Klage beim Zivilrichter zur Durchsetzung ihrer Auskunftsrechte einreichen. Zudem kann bei vorsätzlicher Verletzung der Auskunftspflicht auch eine Strafklage erhoben werden (Art. 34 Abs. 1 DSG).



Das Auskunftsrecht der betroffenen Personen gegenüber dem Dateninhaber einer Datensammlung gehört zu den zentralen Elementen des Datenschutzrechts. Das Auskunftsrecht bezieht sich hierbei auf alle Daten über eine Person in einer Datensammlung, die ihr zugeordnet werden können. Es erstreckt sich auf jede Art von Information, die auf die Vermittlung oder die Aufbewahrung von Kenntnissen ausgerichtet ist, ungeachtet, ob es sich dabei um eine Tatsachenfeststellung oder um ein Werturteil handelt und ob diese Information in einer Datenbank abgespeichert oder nur zur Ansicht jeweils berechnet wird. Entscheidend für die Qualifikation als Personendaten, die vom Auskunftsrecht erfasst sind, ist, dass sich die Angaben einer oder mehreren Personen zuordnen lassen. Wie der Bezug zur betroffenen Person hergestellt wird, ist hierbei ohne Bedeutung. Wesentlich ist, dass die Zuordnung ohne unverhältnismässigen Aufwand möglich ist. Auskunft zu erteilen ist über alle Daten, die sich auf die auskunftersuchende Person beziehen (Art. 3 Bst. a DSG) und die ihr zugeordnet werden können (Art. 3 Bst. g DSG). Wird die Auskunft verweigert, eingeschränkt oder aufgeschoben, muss nach Art. 9 Abs. 4 DSG hierfür ein Grund angegeben werden.

██
██
██
██
██
██
██

██████████ Über die Segmentierungen werden die Cumulus-Kunden mit den Auskunftserteilungen jedoch seit einiger Zeit nicht mehr informiert. Die Einteilung der betroffenen Kunden in entsprechende Kundensegmente stellt jedoch eine wesentliche Komponente der Datenbearbeitung im Zusammenhang mit Cumulus dar. Der auskunftssuchenden Person ist daher mitzuteilen, wie sie aufgrund ihres Einkaufsverhaltens von Cumulus segmentiert wird. Nur so kann sich die betroffene Person ein Bild über die Analyse Kriterien von Cumulus machen und sich in ihrem Einkaufsgebaren entsprechend verhalten. Diese Segmentierungen sind der auskunftssuchenden Person im Sinne von Art. 8 DSG mitzuteilen.

Das Auskunftsrecht wird auf der Webseite von Cumulus unter der Rubrik Datenschutz ausdrücklich erwähnt. Dort findet sich auch ein Formular, wo die betroffene Person Auskunft über die gespeicherten Daten von Cumulus verlangen kann. Auf der gedruckten



Anmeldebroschüre fehlt jedoch ein vergleichbarer Hinweis. Im Sinne der Transparenz soll in oder direkt bei den AGB ein Hinweis auf weitere Informationen und dem Formular über die Auskunftserteilung auf der Homepage abgedruckt werden (vgl. dazu auch Ziff. 5.2 und 12.3).

Zur Gewährung des Auskunftsrechtes wird von der antragstellenden Person eine Kopie eines amtlichen Ausweises verlangt. 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). Der Kunde kann sich daneben den gesamten Warenkorb der vergangenen 2 Jahre anzeigen lassen. Die Kontoabfrage per Internet erfolgt chiffriert, was unter dem Aspekt der Datensicherheit (Art. 7 DSGVO) zu begrüßen ist.

11. Datenauskünfte auf behördliche Anweisung

11.1. 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 Cumulus weitergeleitet. Wenn die Anfrage auf Datenherausgabe gerechtfertigt ist (in Absprache mit der Rechtsabteilung des MGB), liefert 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).

11.2. Bekanntgabe von Kundendaten auf behördliche Anweisung im Einzelnen

Editionsverfügungen werden durch die TELAG und durch Cumulus-Abteilung bearbeitet. Es gibt immer wieder Anfragen von Polizeibehörden (meist wegen Abfallsünder), welche ohne Editionsverfügung Daten verlangen. Solche Anfragen werden jedoch durchgehend verneint.



11.3. Beurteilung aus Sicht des EDÖB

In den AGB zu Cumulus wird in Ziffer 3 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. Der EDÖB begrüsst diese Erwähnung in den AGB ebenso wie die Tatsache, dass strikt keine Daten ausserhalb von Editionsverfügungen an Polizeibehörden bekannt gegeben werden.

12. Datenlöschung auf Verlangen der Kunden

12.1. 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. Cumulus oder an die TELAG resp. das Call Center gerichtet werden. Die Löschanträge werden vom CallCenter bearbeitet und Cumulus übermittelt.

12.2. 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 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 von TELAG haben in diesem Fall strikte Vorgehensanweisungen (festgehalten im DMS-Handbuch) der 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. 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. Mit dem Löschantrag hat der Kunde eine Kopie der Identitätskarte resp. des Passes einzusenden.

Eine Information über das Löschrcht findet sich bloss online auf der Homepage von Cumulus. Darin wird erwähnt, dass die Personendaten nach erfolgtem Löschantrag gelöscht werden.

Migros löscht Stammdaten von sich aus von Cumulus-Mitgliedern, welche während zweier Jahren keine Punkte gesammelt haben. In Ziffer 8 der AGB wird über diesen Sachverhalt informiert. Ebenso werden Kundenkonten mitsamt den angesammelten Punkten unwiderruflich gelöscht bei Kunden, deren Kontoauszüge während zwei Jahren nicht zustellbar ist (vgl. dazu Information in AGB Ziffer 9). Die Löschrungen werden durch IT-Cumulus jährlich jeweils im Januar vorgenommen.

Bei Verdacht auf Missbrauch der Kundenkarte, beispielsweise wenn eindeutig kein typisches Haushalts-Einkaufsverhalten vorliegt, werden die Kontoinhaber der entsprechenden Cumulus-Nummern per eingeschriebenen Brief informiert, dass ihre Karten gesperrt resp. die Daten gelöscht werden. Im Jahr 2014 soll ein systematisches Frühwarn-System eingeführt werden, welches den Missbrauch der Cumulus-Karte feststellen kann. Dabei sollen Auffälligkeiten erkannt und bei gewissen Kriterien reagiert resp. die Mitgliedschaft gekündigt werden. Die Information über die Folgen eines Missbrauchs oder eines Verstosses gegen die Geschäftsbedingungen von Cumulus erfolgt in Ziffer 8 der AGB.

12.3. Beurteilung aus Sicht des EDÖB

Nach Art. 12 Abs. 3 lit. b DSGVO kann eine betroffene Person die Bearbeitung bzw. die weitere Bearbeitung ihrer Personendaten untersagen. Das Aufbewahren und Archivieren stellt eine Bearbeitung im Sinne von Art. 3 lit. e DSGVO dar; eine betroffene Person kann über das Widerspruchsrecht gemäss Art. 12 Abs. 3 lit. b DSGVO die ganz oder teilweise Löschrung von Personendaten beim Inhaber der Datensammlung verlangen. Im Schlussbericht vom 23. Mai 2005 wurde als Anpassungs-/Verbesserungsvorschlag Nr. 3. angeregt, dass das Löschrrecht als fundamentale Rechtsgewährleistung des Datenschutzes in den AGB



erwähnt wird. In den aktuellen AGB wird das Löschungsrecht nicht erwähnt. Auf der Cumulus Homepage jedoch finden sich unter der Rubrik „Datenschutz“ Informationen zur Löschung der Daten und wie der Kunde vorzugehen hat. Diese Informationen sind auch in der Anmeldebroschüre resp. in den AGB aufzuführen (vgl. dazu auch Ziff. 5.2 und 10.3).

Im Schlussbericht vom 23. Mai 2005 wurde angeregt, dass die Information verbessert wird, dass mit einer Konto-Löschung bloss die Stammdaten gelöscht werden. Die Programmdateien werden anonymisiert und sind zu statistischen Zwecken weiterhin zugänglich. Im gleichen Abschnitt auf der Homepage zum Thema Löschung der Daten informiert Migros, dass bei einem Löschantrag die Personendaten gelöscht werden. Auch diese Information ist in der Anmeldebroschüre resp. in den AGB mitzuteilen. Damit wird dem Anpassungs-/Verbesserungsvorschlag Nr. 4 von 2005 genüge getan.

Bezüglich des Frühwarnsystems zur Verhinderung eines Missbrauchs der Cumulus-Karte wird in Ziffer 8 der AGB informiert. Diesbezüglich erscheint die Datenbearbeitung transparent (Art. 4 Abs. 2 DSG) und verhältnismässig (Art. 4 Abs. 2 DSG).

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

13. Aufbewahrung und Löschung weiterer Daten

13.1. Untersucher Datenfluss

Die detaillierten Einkaufsdaten der Cumulus-Mitglieder werden jetzt 24 Monate statt nur 15 Monate aufbewahrt. Begründet wird diese Verlängerung damit, dass der Kunde damit einen längeren Zugriff auf seine Kassabons hat (da die allgemeine Garantie von Produkten 24 Monate dauert) die Speicherkapazitäten bei Cumulus erhöht wurden und für die Datenanalysen eine grössere Zeitbasis zur Verfügung steht.



13.2. Aufbewahrung und Löschung weiterer Daten im Einzelnen

Wie bereits im Bericht vom 23. Mai 2005 festgehalten, werden die Anmeldetalons der Cumulus-Kundschaft 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 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 24 Monaten. Die Einkaufsdaten der Cumulus-Teilnehmer werden nach 24 Monaten gelöscht.

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

13.3. Beurteilung aus Sicht des EDÖB

Die Bearbeitung von Personendaten hat sich am Grundsatz der Verhältnismässigkeit (Art. 4 Abs. 2 DSG) auszurichten. In zeitlicher Hinsicht bedeutet dies, dass die personenbezogenen Daten vernichtet oder anonymisiert werden müssen, wenn sie für den verfolgten Zweck nicht mehr gebraucht werden. Die Erhöhung der Aufbewahrungsfristen der detaillierten Einkaufsdaten von 15 auf 24 Monate erscheint unter dem Aspekt der Garantiefristen und der Erhöhung der Speicher- und Rechnerkapazitäten als verhältnismässig (Art. 4 Abs. 2 DSG).

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. Aus diesem Grund wurde im Schlussbericht vom 28. September 2005 angeregt, dass in den AGB ein Vermerk aufgenommen wird, dass die im Rahmen des Cumulus-Programms erhobenen Daten bis zu 3 Jahre aufbewahrt werden.



Zusätzlich sollen die relevanten Aufbewahrungsfristen im Internet abrufbar sein. Auf den eigentlichen AGB finden sich keine Informationen über die Aufbewahrungsdauer der Cumulus-Daten. Auf der Homepage von Cumulus wird unter der Rubrik „Datenschutz“ informiert, dass die detaillierten Einkaufsdaten 24 Monate aufbewahrt werden und dass die Kassenzetteltotale und Einkaufsprofile maximal 3 Jahre aufbewahrt werden. Ausserdem wird über die Aufbewahrungsdauer gemäss Obligationenrecht informiert. Im Sinne der Transparenz nach Art. 4 Abs. 2 DSG muss direkt bei den AGB auf der Anmeldebroschüre ein Hinweis auf Informationen über die Speicherdauer der Daten angebracht werden.

14. Sicherheit

14.1. Sicherheitsmassnahmen im Einzelnen

Der unbefugte Zutritt zu Räumen, in denen Personendaten bearbeitet werden, wird durch organisatorische und technische Massnahmen geregelt. Die Details dazu finden sich im DMS-Handbuch, welches dem EDÖB vorliegt. Darin werden u.a. auch die Massnahmen zur Verhinderung der Nutzung von IT-Anlagen und Kommunikationseinrichtungen durch Unbefugte, die Verhinderung von unbefugten Zugriffen auf Daten durch berechtigte Systembenutzende und die Verhinderung des Verlustes der Vertraulichkeit, Verfügbarkeit und Integrität während der Bearbeitung von Cumulus-Daten beschrieben.

Im Vergleich zur Sachverhaltsfeststellung von 2005 arbeitet die Abteilung IT-Cumulus nicht mehr in separaten Räumlichkeiten. Um jedoch den gleichen Sicherheitsstandart zu gewährleisten, werden entsprechende Badge-Zutrittsberechtigungen und Passwort-Applikationen sowie individuellen, persönlichen Datenschutz-Schulungen (inkl. jährlichen Auffrischungs-Schulungen) eingesetzt.

14.2. Beurteilung aus Sicht des EDÖB

Gemäss Art. 7 Abs. 1 DSG müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten gesichert werden. Konkretisiert werden diese Anforderungen in Art. 8 ff. der Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (VDSG; SR 235.11). Die organisatorischen und technischen



Massnahmen von Migros erscheinen genügend, um den Schutz der Personendaten zu gewährleisten.

15. Sensibilisierung und Schulung von Cumulus-Mitarbeitern

15.1. Ergriffene Massnahmen und Beurteilung

Da bezüglich der Massnahmen keine Veränderungen zum Schlussbericht vom 28. September 2005 festgestellt werden konnte, kann bezüglich der einzelnen Massnahmen und deren rechtlichen Beurteilung auf die Ziff. 5.11 f. des Schlussberichtes von 2005 verwiesen werden.

Der EDÖB begrüsst das Schulungskonzept und die Sensibilisierungsmassnahmen des MGB im Rahmen von Cumulus sehr und hat dazu keine weiteren Bemerkungen.



16. Ergebnisse

Aufgrund der Auswertung der eingereichten Unterlagen und Dokumente sowie gestützt auf die durchgeführte Kontrolle vom 18. Juni 2013 gemäss Art. 29 DSG, gelangt der EDÖB zu einer überwiegend **positiven Gesamtbeurteilung**. Die Datenschutzkontrolle hat gezeigt, dass die im Rahmen von Cumulus vorgenommene Datenbearbeitung **grundsätzlich datenschutzkonform** verläuft. Trotz dieser überwiegend positiven Beurteilung ist der EDÖB in seiner Datenschutzkontrolle auch auf Sachverhalte gestossen, welche aus datenschutzrechtlicher Sicht einer **Anpassung resp. Änderung bedürfen**. Ausgehend von diesem Gesamtbild erlässt der EDÖB zuhanden des MGB mit Sitz in Zürich seine Gesamtbeurteilung in folgender Form:

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

16.1. Anmeldung

Die Transparenz (Art. 4 Abs. 2 DSG) bei der Anmeldung zum Kundenbindungsprogramm Cumulus ist für die Teilnehmer weitgehend 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.

Im Unterschied zur klassischen Anmeldung mittels Anmeldebroschüre finden sich auf der Homepage von Cumulus wesentliche datenschutzrechtliche Informationen zum Auskunfts- und Löschungsrecht und der Aufbewahrungszeiten der Daten in der Rubrik „Datenschutz“. Diese datenschutzrechtlichen Informationen zu den tragenden Datenschutzrechte sind auch in der Anmeldebroschüre mitzuteilen (vgl. dazu auch Ziff. 10.2, 10.3 und 12.3).

**Anpassungs-/Verbesserungsvorschlag Nr. 1:**

Im Sinne des Transparenzgebots (Art. 4 Abs. 2 DSGVO) schlagen wir deshalb vor, auf der Anmeldebroschüre direkt bei den AGB einen Hinweis auf weitere Informationen und dem Formular über die Auskunftserteilung auf der Homepage abzudrucken (vgl. dazu auch Ziff. 10.2., 10.3 und 12.3).

Bei gewissen Produkten im Rahmen der Aktionen mit „Cumulus-Vorteil“ ist der Kunde auf den Besitz der Cumulus-Karte angewiesen um von dem Preisvorteil zu profitieren. Dies kann unter dem Aspekt der Freiwilligkeit der Einwilligung (Art. 4 Abs. 5 Satz 1 DSGVO) zur Datenbearbeitung resp. Teilnahme am Cumulus-Programm problematisch sein. Die Aktionen sind zeitlich und von der Produktmenge und -wahl derart zu beschränken resp. zu wählen, dass eine echtes Alternativverhalten aus der Sicht der Kundschaft gewährleistet ist, das heisst, dass die Kunden, welche nicht im Besitz einer Cumulus-Karte sind, vergleichbare Angebote auch ohne Cumulus-Karte beziehen können. Aus heutiger Sicht ist dies gewährleistet. Sollten die Aktionen mit „Cumulus-Vorteil“ in Zukunft ausgedehnt werden, kann u.U. nicht mehr von einer freiwilligen Einwilligung und damit von einer rechtsgültigen Einwilligung im Sinne von Art. 4 Abs. 5 Satz 1 DSGVO gesprochen werden.

Anpassungs-/Verbesserungsvorschlag Nr. 2:

Der EDÖB regt an, dass Migros auch in Zukunft sicherstellt, dass sie die Aktionen mit „Cumulus-Vorteil“ zeitlich und von der Produktmenge und -wahl derart beschränkt resp. auswählt muss, dass aus der Sicht der Kundschaft ein echtes Alternativverhalten zur Cumulus-Karte gewährleistet bleibt.



16.2. 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. Die Datenbearbeitung bezüglich Punktesammlung und Spendemöglichkeiten erfolgt verhältnismässig (Art. 4 Abs. 2 DSG).

16.3. Marketing

Im Schlussbericht vom 23. Mai 2005 hat der EDÖB die Empfehlung (Empfehlung Nr. 1) erlassen, dass die Zweckumschreibung bezüglich der Warenkorbanalyse und Marketingauswertungen in den AGB präziser und für den Kunden transparenter formuliert werden soll. In Ziffer 3 der aktuellen AGB informiert Migros, dass „Gestützt auf Ihre Einkaufsdaten bei Unternehmen der M-Gruppe können Warenkorbanalysen durchgeführt werden, die das Konsumverhalten sowie persönliche Personenprofile widerspiegeln können.“ In Ziffer 10 AGB wird informiert, dass die aktuell gültigen AGB jederzeit unter www.migros.ch/cumulus abrufbar sind. Damit wurde die Empfehlung des EDÖB aus dem Schlussbericht von 2005 vollumfänglich umgesetzt.

16.4. Werbung (von Migros)

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. Migros akzeptiert jedoch auch eine Verzichtserklärung zu einem späteren Zeitpunkt; eine Information über die nachträgliche Verzichtsmöglichkeit fehlt jedoch, welche zu ergänzen ist.



Anpassungs-/Verbesserungsvorschlag Nr. 3:

Im Sinne der vollständigen Transparenz über das Recht der jederzeitigen freien Widerrufbarkeit der Einwilligung für Werbung ist hier eine Ergänzung in den AGB anzubringen.

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. Der EDÖB hat deshalb im Schlussbericht vom 23. Mai 2005 die Empfehlung erlassen (Empfehlung Nr. 2), dass bezüglich eines Spezialversandes in der Anmeldebroschüre oder den AGB hingewiesen wird oder dass dieser Versand in Zukunft ganz unterlassen wird. Da die „Aktuell“-Beilage weggefallen ist und kein weiterer Spezialversand festgestellt werden konnte, wurde der Empfehlung Nr. 2 vollumfänglich entsprochen.

16.5. Werbung (von Partnern)

Im Schlussbericht vom 23. Mai 2005 unter Ziffer 5.5.3 wurde festgehalten, dass für die Cumulus-Kundschaft die Möglichkeit der indirekten Datennutzung durch Partnerunternehmen für gezielte Direktwerbung wenig ersichtlich ist. 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 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 EDÖB eine Präzisierung in der Anmeldebroschüre oder den AGB auf. Zugunsten einer vollständigen Transparenz sollen die AGB wie folgt ergänzt werden: „Periodisch unterbreitet die Migros ihrer Cumulus-Kundschaft spezielle



Cumulus-Angebote. Die Teilnehmer stimmen zu, über Cumulus auch Angebote Dritter zu erhalten.“

Anpassungs-/Verbesserungsvorschlag Nr. 4:

Diese Formulierung fehlt in den aktuellen AGB. Wir schlagen deshalb eine Ergänzung vor: „Periodisch unterbreitet die Migros ihrer Cumulus-Kundschaft spezielle Cumulus-Angebote. Die Teilnehmer stimmen zu, über Cumulus auch Angebote Dritter zu erhalten.“

16.6. Auskunftsrecht

Gemäss Art. 8 DSG kann jede Person vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über die bearbeitet werden. [REDACTED]

[REDACTED]

Über die Segmentierungen werden die Cumulus-Kunden mit den Auskunftserteilungen jedoch seit einiger Zeit nicht mehr informiert. Die Einteilung der betroffenen Kunden in entsprechende Kundensegmente stellt jedoch eine wesentliche Komponente der Datenbearbeitung im Zusammenhang mit Cumulus dar. Der auskunftssuchenden Person ist daher mitzuteilen, wie sie aufgrund ihres Einkaufsverhaltens von Cumulus segmentiert wird. Nur so kann sich die betroffene Person ein Bild über die Analysekriterien von Cumulus machen und sich in ihrem Einkaufsverhalten entsprechend verhalten. Diese Segmentierungen sind der auskunftssuchenden Person mitzuteilen.

**Empfehlung Nr. 1:**

Der EDÖB erlässt die Empfehlung, dass der Migros-Genossenschafts-Bund den auskunftssuchenden Personen mitteilt, in welchen Segmentierungen sie aufgrund der Analysen im Zusammenhang mit Cumulus im Zeitpunkt des Auskunftsbegehrens eingeteilt werden.

Das Auskunftsrecht wird auf der Webseite von Cumulus unter der Rubrik Datenschutz ausdrücklich erwähnt. Dort findet sich auch ein Formular, wo die betroffene Person Auskunft über die gespeicherten Daten von Cumulus verlangen kann. Auf der gedruckten Anmeldebroschüre fehlt jedoch ein vergleichbarer Hinweis, welcher zu ergänzen ist.

Anpassungs-/Verbesserungsvorschlag Nr. 5:

Im Sinne des Transparenzgebots (Art. 4 Abs. 2 DSGVO) muss direkt bei den AGB ein Hinweis auf weitere Informationen und dem Formular über die Auskunftserteilung auf der Homepage abgedruckt werden.

16.7. Datenauskünfte auf behördliche Anweisung

In den AGB zu Cumulus wird in Ziffer 3 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. Der EDÖB begrüsst diese Erwähnung in den AGB ebenso wie die Tatsache, dass strikt keine Daten ausserhalb von Editionsverfügungen an Polizeibehörden bekannt gegeben werden.



16.8. Datenlöschung auf Verlangen der Kunden

Eine betroffene Person kann über das Widerspruchsrecht gemäss Art. 12 Abs. 3 lit. b DSG die ganze oder teilweise Löschung von Personendaten beim Inhaber der Datensammlung verlangen. Bei Migros kann ein Cumulus-Kunde auf eigenes Verlangen seine Stammdaten löschen lassen. Die Löschung muss mit einem standardisierten Formular eingefordert werden, welches dem Karteninhaber persönlich nach Hause geschickt wird. Der Antragssteller muss mit seinem Löschungsgesuch eine Kopie der Identitätskarte oder des Passes einsenden.

Das Löschungsrecht als fundamentale Rechtsgewährleistung des wird auf der Cumulus Homepage unter der Rubrik „Datenschutz“ erwähnt und es wird aufgeführt wie der Kunde vorzugehen hat. In der Anmeldebroschüre oder in den AGB finden sich jedoch keine solche Information. Auch über die Folgen einer Löschung, nämlich das bloss die Stammdaten resp. die Personendaten gelöscht werden, wird nur auf der Homepage informiert.

Anpassungs-/Verbesserungsvorschlag Nr. 6:

Der EDÖB regt deshalb dazu an, dass in den AGB oder auf der Anmeldebroschüre über das Löschungsrecht gemäss Art. 15 Abs. 1 DSG, das Vorgehen und die Folgen der Löschung informiert wird.

16.9. Aufbewahrung und Löschung weiterer Daten

Die Erhöhung der Aufbewahrungsfristen der detaillierten Einkaufsdaten von 15 auf 24 Monate erscheint unter dem Aspekt der Garantiefristen und der Erhöhung der Speicher- und Rechnerkapazitäten als verhältnismässig (Art. 4 Abs. 2 DSG).

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. Aus diesem Grund wurde im Schlussbericht vom 23. Mai 2005 angeregt, dass in den AGB ein Vermerk aufgenommen wird, dass die im Rahmen des Cumulus-Programms erhobenen Daten bis zu 3 Jahre aufbewahrt werden. Zusätzlich sollen



die relevanten Aufbewahrungsfristen im Internet abrufbar sein. Auf den eigentlichen AGB finden sich keine Informationen über die Aufbewahrungsdauer der Cumulus-Daten. Auf der Homepage von Cumulus wird unter der Rubrik „Datenschutz“ informiert, dass die detaillierten Einkaufsdaten 24 Monate aufbewahrt werden und dass die Kassenzetteltotalen und Einkaufsprofile maximal 3 Jahre aufbewahrt werden. Ausserdem wird über die Aufbewahrungsdauer gemäss Obligationenrecht informiert. Diese Informationen müssen auch in der Anmeldebroschüre zu finden sein.

Anpassungs-/Verbesserungsvorschlag Nr. 7:

Im Sinne der Transparenz muss direkt bei den AGB auf der Anmeldebroschüre ein Hinweis auf Informationen über die Speicherdauer der Daten angebracht werden.

16.10. Sicherheit

Die organisatorischen und technischen Massnahmen erscheinen genügend, um den Schutz der Personendaten zu gewährleisten.



17. Schlussfolgerungen

17.1. Bezüglich der Kontrolle des Kundenbindungsprogramms Cumulus

Im Rahmen des Kundenbindungsprogramms Cumulus werden Personendaten von einem Grossteil der Schweizer Bevölkerung (es bestehen mehr als 2 Mio. Cumulus-Konten) bearbeitet. Die durchgeführte Datenschutzkontrolle konnte dem EDÖB einen vertieften Einblick in die Abwicklung und in die Datenflüsse im Rahmen von Cumulus liefern. Die von der Migros zur Verfügung gestellten Unterlagen und Dokumentationen haben es dem EDÖB erlaubt, die im Rahmen von Cumulus vollzogene Bearbeitung von Personendaten einer vertieften Prüfung und detaillierten Analyse zu unterziehen und damit die Einhaltung der Datenschutzbestimmungen zu überprüfen. Dem EDÖB hat sich ein überwiegend positives Gesamtbild der Datenbearbeitung präsentiert. Wo Anpassungs- oder Änderungsbedarf besteht, hat dies der EDÖB mit Begründung erläutert.

17.2. Verfahren und weiteres Vorgehen

Es besteht ein grundsätzliches Interesse daran, die Öffentlichkeit für diese Art der Datenerhebung zu sensibilisieren und sie insbesondere über die erfolgte Datenschutzkontrolle bei Cumulus und die diesbezüglichen Ergebnisse zu informieren. Gestützt auf Art. 30 Abs. 2 DSG wird der EDÖB daher den vorliegenden Kontrollbericht betreffend das Kundenbindungsprogramm Cumulus in einer angepassten Version (und bezüglich Namensnennungen anonymisiert) der Öffentlichkeit zugänglich machen und ihn *auf seiner Website (www.edoeb.admin.ch) publizieren*.

Der MGB (Zürich) wird daher aufgefordert, den Kontrollbericht auf solche vertraulichen Inhalte hin zu überprüfen und dem EDÖB **mit Frist von 30 Tagen** entsprechend schriftliche Rückmeldung zu erstatten. Der vorliegende Kontrollbericht enthält eine Reihe von *Feststellungen* sowie *Anpassungs- resp. Verbesserungsvorschläge*, welche vom EDÖB 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 EDÖB **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 EDÖB umgesetzt werden.



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

Mit freundlichen Grüssen

**Eidgenössischer Datenschutz- und
Öffentlichkeitsbeauftragter**

Der stellvertretende Beauftragte

Verfahrensleitender Jurist

Jean-Philippe Walter

Philipp Gisin

Beilagen:

- Empfehlung betreffend die Sachverhaltsabklärung des EDÖB bei Migros betreffend das Kundenbindungsprogramm Cumulus
- Begleitschreiben