ADVERTISING OR SPAM?

Tightened data protection laws and anti-spam guidelines challenge companies in all business sectors. Finding the right balance between corporate marketing goals and compliance with legal requirements is the key to succeed

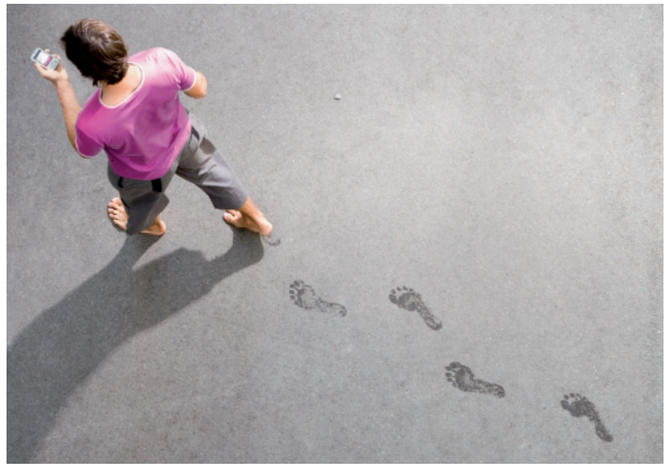
BY **NADINE S. REINFRIED EGLI***

COLLAGE: MARGO PLENGE, PHOTOS: NEWS SERVICE

Topics such as "spamming" and "data protection" are currently on everyone's lips. In the past few years, the number of unsolicited junk mail has increased to a vast amount. The reason behind this trend is that companies increasingly expand their direct marketing measures to attract new customers for their services or to strengthen relationships to existing clients. Direct marketing, however, is a mixed blessing. For the customers concerned, it is usually associated with a bothering element.

A growing number of recipients defend themselves against this rising amount of direct mail by putting a "no advertising" sticker on the mailbox or by an entry in the "Robinson List" (list of contact details for the protection of people who do not want any unsolicited mails and advertising). Finding the right balance between corporate marketing goals and compliance with legal requirements is often a challange. Consumer protection laws are continuously tightened. Since the enactment of the new anti-spam article in the Unfair Competition Act, the legally permitted limit is quickly exceeded.

Companies that maintain a customer database and process customer data also have to comply with strongly tightened privacy regulations which came into effect with the introduction of the current federal act on data protection of 2008. Personal data are a valuable asset which is threatened from all sides and therefore needs protection. Nowadays, companies are able to precisely trace consumer habits of each individual customer by collecting detailed customer data. They are able to create complete personality profiles of individuals to find out what car someone drives, how much he spends on clothes, housing, insurance or holidays. Not ▶



Personal data are a valuable asset which is threatened from all sides and therefore needs protection.

STICKING TO THE RULES

The following are the most important statutory provisions:

Article 3 letter o of the Federal Unfair Competition Act (UCA) bans spam, unfair advertising and sales practices and other wrongful conduct

"Someone is particularly acting unfair by:
sending or arranging to be sent of mass advertising using telecommunications with no direct connection to requested content and in the process omits to obtain the prior consent of customers, to indicate the correct sender or to refer to an easy, free of charge possibility of refusal;
anyone who, when selling goods, works or services obtains a customers' contact information and indicates the possibility of refusal is not acting unfairly if he sends this customer, without the latter's consent, mass advertising for his own similar goods, works or services."

Article 4 of the Federal Act on Data Protection (FADP-Principles):

"1 Personal data may only be processed lawfully.
2 The processing must be carried out in good faith and must be proportionate.
3 Personal data may only be processed for the purpose indicated at the time of collection, that is evident from circumstances, or that is provided for by law.
4 The collection of personal data and in particular the purpose of its processing must be evident to the data subject.
5 If the consent of the data subject is required for the processing of personal data, such consent is only valid if given voluntarily after receiving adequate information. Additionally, an express consent is required in case sensitive personal data or personality profiles are processed."

The media coverage on T-Mobile data loss.

only spying out people, but also data loss – as recently happened with Deutsche Telekom, whose mobile phone subsidiary T-Mobile lost a disk containing personal information of about 17 million of its costumers – is a growing problem. This recent example shows that an early confrontation with sensitive privacy issues is worthwhile and lack of investment in data protection can be devastating. Those companies who do not adapt in a timely manner to the new legal situation face criminal charges and fines. How do customer data have to be protected in order to prevent such charges and fines? Which policies do companies have to comply with in order to strengthen their direct marketing, without falling into the category "spam"? This practitioner's guide gives an overview.

1. The main provisions at a glance

The Unfair Competition Act and the legislation on data protection are closely related. Companies who use direct marketing not only need to comply with the Unfair Competition Act. They also need to exercise particular discretion when handling customer data and private information. And – along the way – they always have to keep an eye on the current data protection provisions. Check the most important statutory provisions on the box "Sticking to the rules".

2. Recent incidents

The loss of customer data by T-Mobile in autumn 2008 has caused a stir and lit up a topic which many companies previously barely focused upon. According to Deutsche Telekom, the lost data not only included names, addresses and mobile phone numbers but, in some cases, also dates of birth and email addresses. Deutsche Telekom didn't directly inform the public about the incident, but merely "filed charges and launched investigations".

Security solution providers criticise the careless handling of sensitive data within certain companies. The primary reason for this problem is the lack of willingness to invest in extensive data protection. Data protection is often perceived as costly, cumbersome and it allegedly hinders business. Consulting lawyers are considered to be detail-obsessed and out of touch with reality. As the example at Deutsche Telekom shows, such an incident can strongly damage the corporate image and the trust of customers in the company. The same applies to aggressive direct marketing which does not always lead to success. All too often good intentions turn into the opposite whereby the company's image can be massively damaged.

Deutsche Telekom promptly reacted to this incident and took exemplary measures to comprehensively protect their data. The development of data protection was a top priority, not least to restore customer confidence.

3. Do's and don'ts

Direct marketing searches for an interactive communication with potential and existing customers, for example by mail, via e-mail, SMS or telephone. In direct marketing the individual customer takes centre stage. The goal is to address the right customer at the right time on the right channel – exactly as he desires. This is the ideal case. In fact, direct marketing does not only target a single customer, but many people are addressed at the same time through mass advertising, regardless of whether they already are a customer or not.

Such mass advertising is only permitted if the following conditions are met:

- The recipient must explicitly consent to receive such mass advertising (approval). This approval must have been given before mailing any advertisements. In addition, the recipient needs to know exactly what he consents to. It is advisable to retain the consent of the recipient in writing (date, duration, scope, possibly signature). When ordering a product online, the recipient only explicitly consents, if he actively approves of receiving product promotion, for example by checking a box:
  ☐ *I would like to receive information about new products and services.*
  ☐ *I would like to receive the monthly newsletter.*

This model is called "opt-in". Not allowed is the so-called "opt-out", which means that a cross is marked by default and the customer has to un-tick the box if he does not want to receive product promotion or advertisements.

There is one exception: An explicit consent of the recipient may also arise from a purchase made with the company, if the purchaser has given the seller its address. In this case the recipient of the advertising is already a customer. The company is allowed to send such a customer advertising for its own products and services of the same type as already ordered.

- The sender of the mass advertising must be named, specifying the correct and complete address details. It is forbidden to conceal the sender.
- Every mailing must include a reference to an easy, free of charge option to refuse future messages. This reference has to be evident and clearly visible. The recipient must have the possibility to immediately refuse any further mailing on the same channel of communication, with no extra effort and cost.

If a company does not comply with these requirements, mass advertising is unfair, violates the law and is classified as spam.

However, even by adhering to these outlined points when sending mass advertising, other problems appear. If ▶

USEFUL LINKS

- Federal Data Protection and Information Commissioner: **www.edoeb.admin.ch**
- Data Protection Officer of the Canton of Zurich: **www.datenschutz.ch**
- Swiss Direct Marketing Association: **www.sdv-asmd.ch**
- Useful information of the Federal Office of Communication (OFCOM) regarding spam: **www.bakom.admin.ch/dienstleistungen/info/00542/00886/index.html?lang=en**
- Consumers against spam – this website explains the topic spamming to consumers: **www.verbraucher-gegen-spam.de**

CHECKLIST DIRECT MARKETING

Explicit consent/approval of the recipient	✓
Correct and complete address details of the sender	✓
Easy and clearly visible option to refuse future messages (same channel of communication, no further costs)	✓
Ensure that customers and email recipients who unsubscribed do not receive further mass emails	✓
No third party advertisements to customers	✓

CORRECT DATA PROTECTION

Compliance with the principle of transparency. Customers need to be informed that data are processed and edited or at least be able to recognise this. In addition, they need to agree to such processing and editing (i.e. with a privacy policy). Minimum information: • What is being processed? • Who processes? • How are the data being processed? • How long will the data be processed? • For which purpose are the data processed? • Reference to inspection and correction rights of customer • Reference to transfer of data and data purchase	✓
Disclosure of personal data to third parties only with the prior consent of the person concerned.	✓
Protection of personal data against unauthorised processing by appropriate technical and organisational measures.	✓

a company maintains a customer database, it additionally has to comply with the data protection requirements. The overarching principle from a legal perspective is transparency. Customers need to be informed that data are processed and edited. In addition, they need to agree to such processing and editing. Companies can get such an agreement by explicitly notifying a customer who makes an online purchase that his address details will be stored and for what purpose the customer's data are used. Often, companies work out a privacy policy which the customer has to accept before disclosing his data. It is advisable to request only those data which are actually needed. Personal data which concern more intimate spheres (i.e. health data) are classified as very sensitive, being subject to even stricter rules. Under certain circumstances, companies even need to register their data collection. In any case, personal data shall only be processed for such purpose for which it was disclosed by the customer or for such purpose which is apparent under the circumstances at hand. A disclosure of personal data to third parties is only allowed if the customer agrees.

While striving to comply with data protection legislation as well as possible, companies further face major organisational challenges. Personal data have to be protected against unauthorised use by implementing reasonable technical and organisational measures. Unfortunately, the security awareness of companies who process data does not often keep up with the technical improvement. Moreover, companies need to raise the awareness of employees and teach them what is important while processing data. Here are some key points regarding the organisational measures a company could take to achieve a comprehensive data protection:

- **Preparation of guidelines:** a first step towards successful data protection is the implementation of a privacy code of conduct for employees.
- **Implementation:** the implementation of the guidelines includes not only sensitisation and education of employees, but also technical protection which focuses on IT-security.
- **Organisation:** regarding organisation, it is advisable to functionally assign areas of responsibility within a company. A central data protection officer coordinates the distribution of tasks and is responsible for keeping track of the current legislation.
- **Control and reporting:** A weekly or monthly report of important incidents and the performance of audits help to prevent major data protection-related incidents.

Another problem area is the international transfer of data. Personal data may only be disclosed to foreign countries if they grant an adequate standard of data protection. With some countries there are agreements in place on this subject (such as the Safe Harbor Agreement with the US).

Data protection and the impact of direct marketing measures are often underestimated. In order not to risk criminal charges and fines, it is advisable to play safe and comply with the obligations. Sanctions for a criminal offense in Switzerland are civil damages, repayment of profit, a prohibition, prison of up to 3 years or a fine of up to CHF 100,000.

Data protection – a competitive advantage?

Compliance with data protection may be a competitive advantage. It surely challenges companies technically, organisationally and financially. However, to prevent damage to the company's image, these challenges should be tackled. The effort which is required to restore the confidence of customers in a company is likely to exceed any preventive measures. If a company is able to establish data protection as a confidence building factor to its customers, it can help to develop a key advantage to its competitors. Switzerland allows companies to stand out with a certification or by appointing a data protection officer. So far, the competitive advantage of data protection is an asset, which develops very slowly, but can quickly be ruined.

** Nadine S. Reinfried Egli, LL.M., is an associate at the law firm MME Partners. Nadine Reinfried's areas of expertise are international and Swiss contract, business and corporate law, data protection law, live entertainment- and ticketing-law and international arbitration. She also advises companies on legal matters concerning direct marketing. For more information, contact her at nadine.reinfried@mmepartners.ch*