

## **Surveying with CustomerGauge - Legal Considerations:**



Adam Dorrell  
09 March 2009 / 12 May 2009 / 3 June 2009

**Please Note – this is not a legal document, and should be used for guidance only. You are advised to seek legal advice before proceeding.**

This document outlines the issues involved in customer surveying, and our understanding of the law as at March 2009.

Contents:

<b>SURVEYING WITH CUSTOMERGAUGE - LEGAL CONSIDERATIONS:</b>	<b>1</b>
<b>GENERAL PRINCIPLES OF CUSTOMER SURVEYING</b>	<b>3</b>
<b>LEGAL ISSUES</b>	<b>3</b>
<b>Avoiding Spam</b>	<b>4</b>
Data Transfer	4
Data Transfer outside the EU	5
<b>DATA SECURITY</b>	<b>6</b>
<b>DATA STORED</b>	<b>6</b>
<b>ANONYMISING DATA</b>	<b>7</b>
<b>BEST PRACTICES</b>	<b>7</b>
<b>ADDITIONAL RESOURCES</b>	<b>7</b>

## General Principles of customer surveying

Our software and service, **CustomerGauge**, is designed to help companies improve their relationship with customers by measuring customer loyalty on several scales (particularly the Net Promoter Score®) and asking open questions about the experience. By processing the results, companies can improve customer experience and grow business. Usually the surveys are conducted by email after a transaction (purchase or support call), or several times a year as part of an ongoing relationship.

It is not in any company's interest to upset or alienate customers, therefore privacy concerns are vitally important for both companies and CustomerGauge.

We have extensively researched the impact of surveying on customers and have concluded that customers are in general responsive to answering surveys. In our experience a high proportion of customers respond (above 25%), and around half are willing to provide constructive comments about service. We have surveyed over 500,000 transactions and in the course have had around 10 (0.002%) negative responses to the survey process, resulting in an "unsubscribe" – and this was due to non-performance on the companies part. We advise some best practices to improve response and reception of surveys at the end of the document.

We believe that companies who listen to customers, and act on the responses are operating a best practice that enhances the relationship.

## Legal issues

We took extensive legal and commercial advice before forming the company. Most companies undertake surveys of some sort without a specific contract clause with their customers, and there are no mentions of surveys in recent EU law. Approaching this from a data privacy point of view is therefore not completely clear.

The laws covering Data Privacy in the EU are based on:

- **Directive 95/46/EC on the protection of personal data**<sup>1</sup>
- **Directive 2002/58/EC** - Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector

Some countries maintain slightly different Data Protection legislation (example Germany: Federal Data Protection Act - Bundesdatenschutzgesetz (BDSG) Stand: 1. Januar 2002)

Key issues involved with surveying:

1. You already have a business relationship with the customer.
2. You have probably surveyed customers before
3. You may already have a clause in your contract that allows for surveying ("We may engage a 3<sup>rd</sup> party to contact you to ask for your opinion"), and if not is a good idea to review that.
4. Collecting customer information on a survey in relation to performance of contract is usually exempt from definitions of unsolicited marketing communications. Example: at the end of a meal, your waiter asks you "Was the food ok?"

---

<sup>1</sup> [http://ec.europa.eu/justice\\_home/fsj/privacy/law/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm)

5. As with any business communication, you should always offer customer the opportunity to “unsubscribe”

## **Avoiding Spam**

Spamming is the sending of unsolicited commercial e-mail. Surveys are not generally considered as spam provided it relates to existing contracts, and the performance of those contracts.

The EU Directive 2002/58/EC on privacy and electronic communications passed in 2002 provides that spamming will only be permissible to individuals who have given prior consent to the receipt of such e-mail. **An exception is provided relating to existing customers, who may be sent the e-mails provided they are given the opportunity to object to future mailings.**<sup>2</sup>

The rules for sending spam to businesses in most countries are less restrictive and essentially require a business to object to such mailings. In certain countries with stricter rules (example Germany) “businesses” and “natural persons” may be treated the same.

Summary of Article 13 EU Directive 2002/58/EC (Email Marketing):

- Email marketing messages can only be sent to natural persons (consumers) who have given their prior consent (opt-in).
- **If there is an existing customer relationship and said customer has not initially refused commercial contact via email, a seller of a product or a service has the right to market to the customer its own similar products or services. In this case, the sender has to offer the recipient a free-of-charge and an easy-to-use mechanism to say no to future emails (opt-out).**
- **It is acceptable to send commercial messages to legal persons (business owners and employees) without prior consent. In this case, the sender also has to offer the recipient a free-of-charge and an easy-to-use mechanism to say no to future emails (opt-out).**
- It is prohibited to disguise or conceal the identity of the sender in a commercial email message.
- It is prohibited not to include a valid address to which the recipient can send a request that further communications cease.

Source: MarketingProfessionals<sup>3</sup>

## **Data Transfer**

It is likely that according to the contract arrangements you have with your customers, you have already asked to process information with third parties (example: Payment Processing, Invoicing, Logistic processing, marketing). This should normally provide permission for CustomerGauge to act as a third-party to collect customer data on your behalf.

---

<sup>2</sup> <http://out-law.com/page-428> - dealing with consumers

<sup>3</sup> <http://www.marketingprofs.com/5/durnik1.asp> - Summary of Article 13

## Data Transfer outside the EU

CustomerGauge is based in the Netherlands (EU). Our data is stored in servers in the EU and the US. You should be aware that in terms of data transfer this could mean that your data may reside outside the EU.

With regard to Directive 95/46/EC (the data protection Directive) and Data-Transfers outside EU: "The principle of the Directive is that personal data can only be transferred to countries outside the EU that guarantee an "adequate" level of protection." The US is sometimes considered to **not** offer an adequate level of protection.

The directive goes on to help companies uncertain of whether a country offers protection: "This could be done by means of a contract between the company sending the data and the non-EU company receiving the data. The object of such a contract would be to provide for adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights. Then, there should be no reason for an EU member state to block any transfer of data relating to its citizens."<sup>4</sup>

Model contracts for the coverage of this are available online<sup>5</sup>.

In any case, there are exceptions:

"... even if the country of destination does not offer an adequate level of protection, data may be transferred in specific circumstances. These are listed in Article 26 (1) and include cases where:

- the data subject has given his or her consent unambiguously to the proposed transfer; or
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party"

We believe that by adding clauses to your standard contract you would be covered under any specific country law on data transfers. You may also choose to view that "the transfer is necessary for the performance of a contract between the data subject and the controller" – which is classified as an exception.

**Update 11 May 2009:** We are now able to offer an EU-only hosting solution for organisations that wish to ensure data resides in the EU. This is offered at a small surcharge to our usual rates.

---

<sup>4</sup> [http://ec.europa.eu/youreurope/nav/en/citizens/services/eu-guide/data-protection/index\\_en.html](http://ec.europa.eu/youreurope/nav/en/citizens/services/eu-guide/data-protection/index_en.html) - Data protection (European Union)

<sup>5</sup> [http://ec.europa.eu/justice\\_home/fsj/privacy/modelcontracts/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm) - Model Contracts

## Data Security

CustomerGauge takes data security very seriously. Steps to ensure this include:

- We have appointed a data protection officer with compliance responsibility.
- Trained all staff who come into contact with personal data. Employees attract personal criminal liability for an unauthorised disclosure of personal data or unauthorised obtaining.
- Identified all third party data processors used by the company. Ensure that data processor contracts are in place.
- Identified all transfers of personal data to EU countries and to third countries. Put appropriate contracts or other compliance methods in place.
- Put in place processes and procedures to identify and satisfy subject access requests (also unsubscribes)
- Put in place processes to deal with requests for disclosure by the Police, Inland Revenue or other Government departments.
- Ensured that IT systems provide adequate security.
- Additionally our websites are tested to check on security breaches and authorised access.
- All site visits are logged with an audit trail of data uploads and downloads.

Our data is only stored in secure servers. Any extracts kept locally are encrypted.

## Data Stored

We request as a data transfer from clients which normally includes:

- Customer ID
- Transaction ID
- Customer Given Name
- Customer Email
- Customer Company Name
- Transaction Value
- Products Purchased
- Transaction Date
- Country of transaction
- Language
- Channel of purchase
- Meta data: Type of purchase (telephone/web)
- Agent/Salesperson Name

We store from customer responses:

- Net promoter Score (0 – 10)
- Additional numeric ratings specific to custom questions
- Open text comments fields
- Multiple choice responses rating to custom questions relating to services
- A “permission to contact” field for follow ups

We provide further database fields to allow adding value to data stored and additional processing (follow up, use for testimonials, workflow etc)

# Anonymising Data

Occasionally, our clients choose to keep their data anonymous for maximum security and confidentiality. When we are asked to do this we do the following:

- Each customer has a reference number provided by the company. We cannot track this back to any company data.
- We do not use names for an organisation or a person – again, reference numbers only.
- All segmentation details are masked – for example: instead of “employees, staff, public” it is A, B, C, D or H1 H2, L3 L2.
- Any other information can be masked – sometimes we have revenue numbers. This can be represented by code words “Red / Orange / Blue”

After we have done an email pass, we can delete email addresses too. At all times, our clients own the data and can download it at any time. We are able to delete the data we store at any time.

## Best practices

- Appoint a privacy officer
- Review contract with customers – add provision for surveying and data transfer
- Explain to customers early in the purchase process that they will be surveyed to help company perform better
- Politely ask to complete survey by email or other emails
- Keep survey short (less than 2 minutes to complete)
- Offer opportunity to unsubscribe
- Do not over-survey (2x a year is probably maximum)
- Make sure all customer comments are answered promptly
- Publish results of surveys to customers to show that input is valued (anonymising results)

---

## Additional Resources

### Consumer protection (Germany)

Germany passed an e-commerce law that implements the EU e-commerce directive, with effect from December 2001 (Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr, BGBl. I 2001 S. 3721). It strengthens consumer protection and privacy, thereby tightening the 1997 electronic-data-protection law. The latter was superseded in March 2007 by a new law on electronic media (Telemediengesetz, BGBl. I 2007 S. 179) that streamlines various laws and regulations concerning online services and e-commerce.

Under its provisions, e-commerce companies must inform their customers if they collect personal data that enables the customer to be identified. Customers must consent in writing for their data to be used for advertising purposes. If the user revokes the agreement, the e-commerce company must delete the data. Otherwise, the company may collect personal data only for billing purposes; moreover, it must ensure that third parties do not gain access. The new law allows the authorities to demand that the service provider hand over personal data if these are needed for criminal prosecution, prevention of hazards or enforcement of intellectual-property rights.

The law also sets strict rules requiring e-commerce firms to provide extensive information about themselves on their websites, ranging from address and telephone contacts to their tax-registration numbers. Moreover, it sets rules about unsolicited e-mail advertising, or spam, which is illegal unless the consumer agrees to receive such mail. E-mail advertising must also be labelled as such in the subject heading. Privacy violations and the sending of spam are subject to fines of up to €50,000. Disputes involving consumer rights are dealt with by courts in the buyer's country of residence.

A law on the sale of financial products via the Internet, telephone or fax, entered into effect in December 2004, transforming an EU directive of 2002 into national law. The law requires financial-service providers (such as credit-card companies or mutual funds/unit trusts) to inform potential customers of prices, payment, contract law and risks before a contract is signed. The customer has the right to withdraw from a contract until 14 days after its conclusion (30 days for pension insurance, zero days for price-sensitive deals such as currency trading).

Banks have warned about attempts to steal account and PIN numbers (known as “phishing”) from online banking customers. Banks have responded by introducing indexed transaction numbers. Under this system, a specific number from a list of numbers previously handed to the bank customer must be entered upon prompt before a banking transaction can be carried out. Alternatively, a transaction number can be individually sent to a previously assigned mobile phone.

The Voluntary Self-Control of Multimedia Service Providers (Freiwillige Selbstkontrolle Multimedia-Diensteanbieter—www.fsm.de) is an association that promotes self-regulation of service providers under a shared code of conduct. It offers a complaint office that can take action against its members. Membership is voluntary.

Source:

[http://globaltechforum.eiu.com/index.asp?layout=rich\\_story&channelid=4&categoryid=29&title=Germany%3A+Overview+of+e-commerce&doc\\_id=11163](http://globaltechforum.eiu.com/index.asp?layout=rich_story&channelid=4&categoryid=29&title=Germany%3A+Overview+of+e-commerce&doc_id=11163)

Model Contracts: [http://ec.europa.eu/justice\\_home/fsj/privacy/modelcontracts/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm)

Contract and directive: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:EN:PDF>

## **UK Law**

*from Information Commissioner's Office (the UK's independent authority set up to promote access to official information and to protect personal information) - <http://www.ico.gov.uk/>*

From FAQs:

“The Privacy and Electronic Communications Regulations lay down rules for organisations sending unsolicited marketing by electronic means. The rules are different depending whether the recipient is an 'individual subscriber' (e.g. Jonsmith@yahoo) or a 'corporate subscriber' (e.g. Jonsmith@ico).

The regulations say that organisations must have prior consent to send unsolicited marketing material by electronic mail to individual subscribers, **unless they have obtained the details during the course of a sale, or negotiations towards one, and they give you the opportunity to object in every message.** If you are an individual subscriber receiving unsolicited marketing by electronic mail, and the organisation hasn't stopped even though you've tried to opt out, you can complain to the ICO.

If you are a corporate subscriber the prior consent rule does not apply. Marketing communications should still identify the sender and provide a valid address. Depending on the information the company holds about you, a corporate subscriber may also have rights under section 11 of the Data Protection Act 1998.”

[http://www.ico.gov.uk/Global/faqs/privacy\\_and\\_electronic\\_communications\\_regulations\\_for\\_the\\_public.aspx#F0FFE5E6-F4F4-49C5-A43A-6448C4CB1B44](http://www.ico.gov.uk/Global/faqs/privacy_and_electronic_communications_regulations_for_the_public.aspx#F0FFE5E6-F4F4-49C5-A43A-6448C4CB1B44)

**CustomerGauge interpretation is that if a valid relationship is in place then surveying customers should be completely acceptable.**

---