Eloqua Whitepaper
Compliance with EU Data Protection Requirements

1.	Overview	4
2.	European Union Data Protection Law	5
2. 1	EU Data Protection Legal Framework	5
2.2	EU Data Protection Legislation in Member States	5
2.3	Which law applies?	6
2.4	Who is responsible for compliance, Eloqua or the Customer?	7
2.4.1	Processing by a third party	7
3.	Requirements of Lawful Data Processing in the EU	8
3.1	Principles of the Directive	8
3.2	When can personal data be processed?	9
3.3	Informed Consent	9
3.3.1	Consent Defined	10
3.3.2	Consent from Minors	10
3.3.3	Other forms of justification	10
3.4	Use of Personal Data for Direct Marketing Purposes	11
3.5	Transfer of Personal Data	11
3.6	Sensitive Personal Data	12
3.7	Administrative Requirements	12
3.7.1	When do I need to notify the appropriate authorities?	12
3.8	Enforcement	12
4.0	Data Protection Legislation in Germany	13
4.1	Legal Framework	13
4.2	When does German Law apply?	13
4.3	Can Eloqua be configured to properly comply with German Data Protection Law?	13
4.4	User Tracking, Script and Cookies	13
4.5	Opt-in for e-mail Newsletters	14
4.6	Notification and Data Protection Official	14
5	Legal Guidelines on Drafting and Obtaining Consent	14
6.0	Case Studies	15
6.1	Case 1: Eloqua customer based in the USA, are they required to comply?	15

© 2011 Eloqua Corporation. All rights reserved.

6.2 Case 2: Website Tracking and Personal Profiles 16
6.3 Case 3: Confirmed Opt-in 16
6.4 Case 4: Sending tracked e-mails from Outlook using Eloqua for Microsoft Outlook 16
7.0 Resources 17
7.1 Visitor Tracking Opt Out Instructions 17
7.2 Confirmed Opt In Process 18
7.3 Manage Subscriptions 18
7.4 Master Exclude List 18
7.5 Form Layout 18

© 2011 Eloqua Corporation. All rights reserved.

Legal Disclaimer

Note that the purpose of this Whitepaper is to provide general information about basic principles of data protection law in the European Union. **It does not constitute legal advice** and Eloqua does not accept any liability regarding its completeness, accuracy or relevance.

Please consult your own legal counsel prior to implementing corporate compliance policies and associated solutions using Eloqua Conversion Suite.

Have additional questions?

For non-legal requests or questions concerning EU compliance, member state compliance or configuring Eloqua for compliance, please contact your Customer Success Manager and they will be happy to assist.

© 2011 Eloqua Corporation. All rights reserved.

1. Overview

Over the past few years, marketers have been faced with increasing pressure to ensure emails ended up in their recipient's inbox. SPAM and deliverability were and continue to be hot topics on many marketers' minds. However, over the last few years, a new issue has become particularly important throughout the global, but more in particular the European region, compliance.

As hype and anger over SPAM reached top levels of government through the last decade, data protection laws were changed, enhanced, or new laws put in place to try and curb this mass marketing practice, typically used to promote scams and illicit material.

In 2003, the U.S. government introduced CAN-SPAM, a dedicated law designed to combat SPAM by setting out specific guidelines for marketers and subsequent penalties/fines for those who are reported as SPAM and do not comply.

In the European Union, a similar but stronger response was implemented. Already in place was the 1995 EU Data Directive covering processing and transport of a person's data. However, the need for an accompanying law to tackle the rapidly expanding electronic communications medium was necessary. Intro the 2002 EU E-Privacy Directive, covering protection and privacy in electronic communications. To complicate matters further, some EU member states implemented their own compliance and SPAM laws, which if deemed stricter than EU law would supersede EU law in a court of law.

With all the various laws and differences between EU member states, it has made it very difficult for marketers to easily understand what they can and can't do to collect, store and market to their recipient base.

The following whitepaper aims to address these concerns from both a North America and EMEA perspective, and to provide a quick reference to the tools available in Eloqua that enable compliance.

NOTE: This current version focuses on EU specific law and German Data Protection law, which is considered the strictest in the EU. Since German law is the strictest, the solutions provided in this document will be sufficient to cover legal privacy requirements in any other EU member state. Eloqua recommends that you familiarize yourself with the local laws of each member state via your legal team and by using resources such as:

http://www.bakermckenzie.com
http://www.nymity.com/
https://www.privacyassociation.org/

Over time, this document will be updated with specifics on additional countries and associated best practices.

© 2011 Eloqua Corporation. All rights reserved.

2. European Union Data Protection Law

2. 1 EU Data Protection Legal Framework

European data protection legislation is based on several Directives, the most important and relevant one being **Directive 95/46/EC** (on the protection of individuals with regard to the processing of personal data and on the free movement of such data) and 2002/58/EC (concerning the processing of personal data and the protection of privacy in the electronic communications sector)[1]. These Directives are the basis for the data protections laws in all EU member states[2] and regulate the processing of personal data.

Personal data, according to the Directive is data consisting of information that relates to a natural person who can be identified from that information (or from that and other information in the possession of the data user). Almost any data about someone can be personal data, including name, age, gender, private address, business address or e-mail address as well as the behavior connected to that individual.

Processing of personal data means any operations, which are, performed upon the personal data, including collection, recording, organization, storage, alteration, retrieval, use, disclosure by transmission or otherwise making available, combination or erasure. The person or company responsible for the processing of personal data is called the **data controller**.

2.2 EU Data Protection Legislation in Member States

European Directives are binding only for the member states and need to be implemented into the **national law of each member state**. As the EU Data Protection Directives only specify minimum measures, member states are free to implement stricter requirements. This has resulted in inconsistencies between national data protection laws as well as interpretation of the Directives across the EU. Most of these inconsistencies relate to administrative requirements such as whether or not a data controller must appoint a personal data protection official or whether the data processing activities need to be registered with the member states local data protection authority.

However, in some member states, differences concern the data protection law itself. For example, whereas in most countries the term "personal data" only covers data relating to living individuals and not data relating to other legal entities, in Italy data protection laws also apply to deceased individuals and corporate entities.

The following paragraphs focus on the EU Directive itself and do not focus on special member state requirements. In section 4 of this whitepaper, special requirements and interpretations related to German law are discussed.

[1] Both Directives are available online on the website of the European Commission: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

[2] European Union has several member states which can be found here: http://europa.eu/abc/european_countries/index_en.htm

© 2011 Eloqua Corporation. All rights reserved.

Over time this whitepaper will be expanded to include additional member state requirements that differ from EU and German law. It should also be noted that Germany was chosen due to their extremely strict data protection law.

2.3 Which law applies?

Directive 95/46/EC stipulates that for data protection laws of a particular member state to apply to the collection of personal data by means of a website, the data controller (which, in the context of online collection, will usually be the website operator) is required either to be established in that country or to use equipment within that member state in order to process the personal data. Therefore, use of servers in a particular country to host a website, whether operated by the collecting entity itself or its ISP may count as the "use of equipment" within that country, even if the website operator is not "established" in that country. In some member states, the view has been expressed that the mere placing of a "cookie" on the computer of a user physically located in that member state may amount to the use of "equipment" within the relevant EU member state. If the data controller operates establishments in several member states across Europe than it has to ensure that it complies with the local data protection laws in all those member states.

Alert

The European Union adopted new changes to the EU Directive at the end of December 2009 to make consent required for placing a tracking device or technology onto someone's computer such as a cookie, flash, or beacon. This change must be enacted by Member States by Summer 2011. Eloqua is aware of these changes and is working to develop new technology to enable easy compliance in advance of this change.

Generally, EU data protection requirements have to be taken into account if;

1. Data is collected, processed in or through an **'establishment' located in any EU member state** (being a branch office, subsidiary or any other 'effective and real exercise of activity through stable arrangements as defined by Directive 95/46/EC).
2. If no such establishment exists in a member state then EU data protection law still applies if data is processed **using equipment located in the EU**, in particular a server.
3. The **national data protection law in some member states** provides for even stricter requirements. In Denmark, for example, the Danish Data Protection Act explicitly stipulates that the Danish Data Protection Act is applicable if the personal data is collected for the purpose of processing outside of the EU[3]. That means that Danish data protection law practically applies to any collection of personal data in Denmark, even if done through a web server outside of the EU.
   Therefore if neither 1 nor 2 apply, local law in the particular member state has to be checked in order to exclude the applicability of EU data protection law.

[3] Article 4 (3) No. 2 of the Danish Data Protection Act (Act No. 429 of 31 May 2000).

© 2011 Eloqua Corporation. All rights reserved.

2.4 Who is responsible for compliance, Eloqua or the Customer?

2.4.1 Processing by a third party

Technically, Eloqua collects and stores personal data of users/web visitors. However, per the Eloqua Master Agreement, Eloqua is provided as a service, collecting data on behalf of the customer with the customer 'owning' the data. It is the customer who decides what the processing will be and how handling of the collected data should be implemented.

According to the EU Directive definition, the customer is considered as data controller and **Eloqua is acting as the data processor**. Therefore, the customer has to ensure compliance with data protection laws and Eloqua must comply with the written instructions of the data processing agreement that is integrated into the Eloqua Subscription Agreement between Eloqua and the customer. Note that in Germany, the law requires an additional agreement between the Data Controller and Data Processer.

The same is true for any third party processing of personal data on behalf of the data controller, e.g. the ISP which is hosting the website or a service provider sending out letters to users on behalf of the customer.

© 2011 Eloqua Corporation. All rights reserved.

3. Requirements of Lawful Data Processing in the EU

3.1 Principles of the Directive

As stated above, requirements on lawful processing of personal data may vary in the individual member states. However, **principles of the Directive 95/46/EC apply to the local data protection law in all EU member states**:

- Personal data must be processed fairly and lawfully.
- Personal data must be collected for explicit and legitimate purposes and used accordingly.
- Personal data must be relevant and not excessive in relation to the purpose for which they are processed.
- Personal data must be accurate and where necessary, kept up to date.
- Data controllers are required to provide reasonable measures for data subjects to rectify erase or block incorrect data about them.
- Personal data that identifies individuals must not be kept longer than necessary.

Further, the data controller has to provide the following information to the individual, unless the individual is already aware of the respective information:

- The identity of the controller and of his representative, if any
- The purposes of the processing for which the data are intended
- The categories of data captured
- In case of an intended transfer, recipients or categories of recipients
- Possible consequences if the data is not disclosed by the individual
- Existence of the right to access, right to rectify and right to remove data concerning the individual if/when necessary
- Outlining specific circumstances in which data is collected, guaranteeing fair processing with respect to the data subject.

Recommendation

The above 7 bullet points provide a good outline of specific items to include in your corporate Privacy Policy. Note that these items should not necessarily replace your current Privacy Policy but append if not covered in your current version. **An example Privacy Policy can be found at the bottom of our website at** http://www.eloqua.com.

© 2011 Eloqua Corporation. All rights reserved.

3.2 When can personal data be processed?

Within the EU, a data controller is required to justify the processing (e. g. the collection and further use) of personal data before it will be considered lawful. According to the Directive, processing of personal data is lawful if:

1. The individual has unambiguously given his or her consent, i.e. if he or she has agreed freely and specifically after being adequately informed.
2. Data processing is necessary for the performance of a contract involving the individual or in order to enter into a contract requested by the individual, e.g. processing of data for billing purposes or processing of data relating to an application i.e. job posting or loan.
3. Processing of personal data is required by a legal obligation.
4. Processing of personal data is necessary to protect an interest that is essential for the data subject's life. For instance, in the case of a car accident and the data subject is unconscious, emergency paramedics are allowed to give blood tests if it is deemed essential to save the data subject's life.
5. Processing is necessary to perform tasks of public interest or tasks carried out by official authorities (such as the government, the tax authorities, the police etc.).
6. Processing is necessary for the purposes of legitimate interests pursued by the controller, except where such interests are overridden by fundamental rights and freedoms of the data subject. This provision establishes the need to strike a reasonable balance between the business interest of the data controller and the privacy of data subjects.

With respect to processing personal data for general marketing purposes - only consent (1), permission regarding the performance or the entering into a contract (2) or the legitimate interests of the controller (6) will be deemed relevant for lawful processing of personal data.

3.3 Informed Consent

To satisfy data protection law requirements, in most countries, obtaining **informed consent of the data subject** at the time of personal data collection will be sufficient. Even though it is not the only option for lawful processing of personal data, obtaining the consent of the data subject is often the simplest means of doing so.

© 2011 Eloqua Corporation. All rights reserved.

3.3.1 Consent Defined

EU Data Directive defines consent as "any freely given, specific and informed, indication of an individual's wishes by which the data subject signifies their agreement to processing of personal data[4]".

With regard to form and content of such consent or opt-in, **most member states do not require the consent to be given in writing**. However, some countries (like Germany, see below) introduced **stricter requirements for consent given online**.

3.3.2 Consent from Minors

For some customers, questions may arise as to the reliability of consent obtained from minors. The EU Data Directive does not address this issue directly. However, in some member states specific rules apply. If through your marketing efforts you may collect consent from minors, it is recommended that you review the relevant local data protection laws that apply.

3.3.3 Other forms of justification

A consent is not required if the processing is necessary for the purpose of the **performance of or the entering into a contract with the individual**. However, this requires that the (intended) agreement actually be between the individual and the customer, not, for example, between the employer of the individual and the customer. Even if the agreement is between the individual himself and the customer, processing is only covered to the extent required for the performance of or entering into the agreement. A typical example would be where a website operator processes details of a customer's address for the purpose of delivering goods ordered from its online store. In most member states the purpose of "entering into an agreement" is interpreted with a very narrow view and does not include general marketing to individuals.

The same is true for the **"purposes of the legitimate interests pursued by the data controller"**. Under most local data protection laws, marketing of your products or services to prospective customers is not a sufficient basis for processing of their personal data.

Therefore, obtaining consent or opt-in remains the best way of achieving across all EU member states.

Tip!

For information on configuring Eloqua to comply with EU consent guidelines please see the instructions listed in section 7 of this document or contact your Customer Success Manager.

[4] Articles 2(h) and 7(a) of Directive 95/46/EC.

© 2011 Eloqua Corporation. All rights reserved.

3.4 Use of Personal Data for Direct Marketing Purposes

EU legislation intentionally makes using personal data for the purposes of direct marketing more difficult. The Electronic Communications Directive 2002/58/EC generally prohibits marketing activities conducted via automated calling machines, fax or e-mail, unless prior **explicit** consent of the relevant recipients has been obtained[5]. However, according to the Directive, when an e-mail address has been obtained from a user in relation to the sale of a product or service to this same user, in accordance with Directive 95/46/EC, this **e-mail address may be used by the customer for direct marketing** of its own similar products or services, provided that the users "clearly, and distinctly be given the opportunity to object, free of charge, and in an easy manner, to such use of electronic contact details when they are collected, and on the occasion of each message in case the customer has not initially refused such use".

Under the EU Data Protection Directive, individuals have the right, at any time, to withdraw permission for receiving future marketing materials[6]. For this reason, it is recommended that a **separate marketing communications consent** be completed using either telephone, fax or e-mail as the point of collection. This process should also be carried out even if the use of the individual's personal data would otherwise be justified (e. g. the conclusion of an agreement, see above).

3.5 Transfer of Personal Data

According to the directive and all EU national data protection laws, transferring of personal data to a third party (other than a data processor) **is** also considered processing. For transferring data within the EU and the associated countries of the European Economic Area (EEA) (Norway, Liechtenstein and Switzerland) no additional restrictions apply. However, it is generally prohibited to transmit data to countries outside the EEA that do not ensure an "adequate level of protection". To date, only a small number of countries have been accepted by the European Commission as to providing such an adequate level of data protection, **Canada** being one of them[7]. Because Eloqua's technical infrastructure/data centre is located in Toronto, Canada, no specific requirements for transferring to and from the EEA are necessary.

NOTE: For transferring data to any other entity (including intra-group transfer) it is necessary to:

- Obtain consent of the individual that the data is being transferred to a country which does not provide an adequate level of protection (according to EU)
- Conclude a contract between transmitting and receiving party, which obliges the recipient to observe certain safeguards. Note, the EU has approved standard clauses that comply with these legal requirements and are available for use in contracts
- Intra-group transfers may also be justified, if the company adopts a specific set of rules that ensure data protection across all companies within the group, whether located in or outside the EEA. These rules need to be approved by the data protection authority in each member state from which the company intends to transfer data.
- For USA based companies, signing up to the **Safe Harbour** program is an additional option http://www.export.gov/safeharbor/.

[5] Article 14(1) of Directive 2002/58/EC.
[6] Article 14(b) of Directive 95/46/EC.
[7] Besides Canada, only Argentina, Isle of Man and Guernsey have been approved so far.

© 2011 Eloqua Corporation. All rights reserved.

3.6 Sensitive Personal Data

With respect to sensitive data, special rules may apply depending on member state law. These laws apply to personal data deemed "sensitive" such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life.

In principle, such data cannot be processed. The Directive tolerates exceptions under very specific circumstances. These circumstances include the data subject's explicit consent to process sensitive data, the processing of data mandated by employment law, where it may be impossible for the data subject to consent (e.g. blood test to the victim of a road accident), processing of data has been publicly announced by the data subject or processing of data about members by trade unions, political parties or churches. Member states may provide for additional exceptions for reasons of substantial public interest.

Generally, sensitive data should not be processed. If you choose/require collection of sensitive data, a detailed review of the requirements against the various member state data protection laws will be necessary. Note that the Eloqua Master Subscription Agreement explicitly prohibits collection and storage of sensitive data.

3.7 Administrative Requirements

According to the Directive, all data controllers must **notify the local supervisory authorities** when processing data. Member states may provide a simplification or exemption from this notification requirement; several states have done so, Germany being one of them. This requirement does not apply to any processing activities that are subject to EU data protection law. However, if you are subject to such notification requirements it may be required, depending on the local law, to also include Eloqua's services in such notification[8]. If so, **please notify your Solutions or Customer Success Manager** so that we are aware of this requirement.

3.7.1 When do I need to notify the appropriate authorities?

Member state authorities must be informed by the data controller **before** commencing automated processing of personal data. Depending on national legislation this notification may be substituted by the **appointment of a personal data protection official** within the entity. This person ensures, in an independent manner, the internal application of data protection law and keeps a register of processing operations carried out by the controller. This register will also contain the items of information referred.

3.8 Enforcement

There is no central European data protection agency. National data protection laws are enforced by the data protection authorities of the individual member states and through the European Data Protection Supervisor. Therefore, as one might imagine, levels of enforcement activity across these organizations vary from country to country.

[8] Extensive guidelines (the 'Vademecum') on member state notification requirements are available online at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2006-07-03-vademecum.doc

© 2011 Eloqua Corporation. All rights reserved.

4.0 Data Protection Legislation in Germany

4.1 Legal Framework

In Germany, the Federal Data Protection Act (Bundesdatenschutzgesetz -BDSG) applies. BDSG implemented the EU Data Protection Directive 95/46/EC which took effect on 23 May 2001. In July 2009, a second amendment to BDSG, Commissioned Data Processing (Auftragsdatenverarbeitung) was passed which requires a contract between a Data Controller and it's Data Processor. The contract must detail the types and scope of the processing to be undertaken. Eloqua has a model contract available for this purpose. Speak to your Solutions or Customer Success Manager for more information. In an online context, the German Federal Tele Services Data Protection Act (Teledienstedatenschutzgesetz - TDDSG) is also applicable. Direct marketing is subject to the German Act on Unfair Competition (Gesetz gegen unlauteten Wettbewerb - UWG) which also implemented some of the Directive 2002/58/EC requirements.

Due to the federal structure of Germany, no single German data protection authority exists; interpretation and enforcement of the Data Protection Act depends on 16 separate state (Länder) authorities. Therefore, interpretation and level of enforcement sometimes vary.

4.2 When does German Law apply?

In accordance with the Directive, German Federal Data Protection Act applies if the data controller operates an establishment in Germany or is using equipment located in Germany for the collection and use of personal data. According to some Länder data protection authorities, even the use of JavaScript or cookies on the user's PC (if they contain personal data or help to reveal the identity of the user) is considered sufficient. However, **the German authorities have no actual jurisdiction over foreign data controllers** and therefore have no means of actually enforcing compliance.

4.3 Can Eloqua be configured to properly comply with German Data Protection Law?

Yes. The German Data Protection Act allows the collection, processing and use of personal data if either a legal provision approves it or the individual has given his **consent**. In an online environment, such consent may also be given in electronic form. In order for **electronic form** consent to be valid, it has to be ensured that:

- such consent can be given only through an unambiguous and deliberate act by the user,
- consent cannot be modified without detection,
- the creator can be identified,
- consent is recorded
- text of the consent can be obtained by the user on request at any time.

4.4 User Tracking, Script and Cookies

Tracking the behaviour of known users on a website will require prior informed user consent. The same is true when using scripts or cookies which identify the individual user. Such consent has to be clear about the extent and purpose of the collection and processing of personal data. If a user accesses a website for the first time it is sufficient to have a privacy notice (Datenschutzerklärung) on the website explaining the user is being tracked and

© 2011 Eloqua Corporation. All rights reserved.

that cookies are being used etc. However, as the user identifies themselves by signing up for a newsletter, service etc. and Eloqua, from that point forward, tracks on an individual and identifiable level, then consent is required unless you have any other legal basis for the tracking to exist (e. g. the tracking is part of the service the user has signed up to).

4.5 Opt-in for e-mail Newsletters

The German UWG requires an opt-in procedure for sending commercial communication by e-mail to users. In fact, several court decisions have effectively created a confirmed opt-in requirement (see case study 4 below).

Direct marketing to consumers via telephone are considered to be harassment if the consumer hasn't given prior consent, whereas calls to business contacts are legitimate if an objective interest of the addressee based on circumstances can be assumed (opt-out).

4.6 Notification and Data Protection Official

Generally, **no notification** is required under German data protection law. However, every data controller having more than 9 employees working on processing of personal data must appoint an internal or external **data protection official**. Primary duty of the data protection official is to ensure internal compliance of the data processing activities.

5 Legal Guidelines on Drafting and Obtaining Consent

For valid consent to be given online, it must fulfill the following requirements:

1. Text of the consent form should be in **plain language** rather than using legal speak; wording should be phrased not as an agreement but as an acknowledgment of information which will not be considered as freely given if the individual does not understand.
2. The **data controller has to be identified**
3. Must outline the **type of data** collected and how it is done.
4. **Purpose for processing** an individual's data must be identified; the consent will only be valid for processing activities which are covered by the purpose(s) identified to the individual at the time of consent.
5. It has to be ensured that the user is giving the consent **prior** to the collection of personal data;
6. Safeguards should be in place to **prevent giving of consent by mistake** (i.e. do not use pre-checked boxes);
7. Information about the **consequences of not consenting** must be given (i.e. that the service may or cannot be used or only limited functions are available etc.)
8. Brief **explanation of the rights of the user,** outline that the user has the right of access to and the right to rectify their data. It is recommended that a point of contact be listed where the user can request access to their data.

© 2011 Eloqua Corporation. All rights reserved.

6.0 Case Studies

6.1 Case 1: Eloqua customer based in the USA, are they required to comply?

Question: A company based in the USA is targeting EU customers. The website is hosted in the USA and the US Company has no offices up and running in the EU. Are Eloqua customers required to follow EU data protection laws if Europeans are visiting the USA hosted website?

The EU Data Protection Directive requires that a member state's law apply if the data controller, for purposes of processing personal data, makes use of equipment, automated or otherwise, which is situated within a member state. This is true, irrespective of the fact whether the USA based company has **signed up to Safe Harbour or not.**

NOTE: This scenario also applies to all non-EU countries, including countries which according to the EU Commission, offer an adequate level of data protection i.e. Canada .

If the website is hosted outside of the EU and the foreign company is not using any other equipment located in the EU, nor has any form of establishment in the EU, most member states will not apply their data protection law. However, some member states (including a considerable number of German data protection authorities) argue that using cookies and scripts on the PC of the user (located in the EU) would constitute the use of "equipment" under the Directive.

Some countries, like e.g. Denmark always declare the local data protection law as applicable if the data is collected for the processing of data outside the EU.

Question: If the US Company has a .de (or any other European) site but the pages are hosted in the US does it change anything?

No, the domain name or respective top level domain itself has no influence on the applicability of European data protection law. However, registering a country code top level domain requires naming at least one administrative contact (admin-c) in the respective country. Some member states may consider this as a local "establishment" and may apply data protection law.

Question: If the customer has a ".de" (or any other European) site that is hosted in Europe but the company is US based does this change anything?

Yes. Operating a server in the EU is considered as either establishment, or the use of equipment located in the EU. Local data protection law will apply in most member states.

© 2011 Eloqua Corporation. All rights reserved.

6.2 Case 2: Website Tracking and Personal Profiles

A German based Eloqua customer is using website integration, what must the company display on a form or in an e-mail to ensure compliance?

The user has to declare his consent prior to the collection of his/her personal data. If the customer is collecting, processing or using personal data by tracking the behaviour of users on their website, the customer needs to have a legal basis for doing so. However, as long as the customer has not signed up to service or registered on the website and remains anonymous. As soon as the click stream data is being linked to a specific user, e.g. because the user has identified themselves or signed up to a service, consent is required. If the click stream is only linked to a certain company (e. g. the company proxy server) and does not relate to an individual, data protection law in most member states will not apply.

How should this be implemented?

The user must actively check a box that explicitly outlines what he/she is consenting to.

6.3 Case 3: Confirmed Opt-in

Website contains a whitepaper download form that once submitted, sends the visitor an e-mail with a link to download a whitepaper.

As the recipient has requested the whitepaper the e-mail containing the download link is not considered "unsolicited communication" under the Directive 2002/58/EC or the respective German law. However, it is the sender's obligation to ensure that only the actual person requesting the whitepaper is receiving the e-mail. Therefore, several German courts have requested that the sender use a Confirmed opt-in procedure for signing up to newsletters or other commercial communication. This means that the recipient receives a short e-mail confirming that he has requested to receive a certain newsletter; the recipient then has to actively confirm this e-mail either by clicking on a hyperlink or by replying to the e-mail. This process prevents third parties from 'signing up' other individuals.

However, for one-time e-mails where only a single e-mail is being sent, this confirmed opt-in procedure seems not to be applicable as it does not prevent the receipt of the first e-mail. Nevertheless it remains the responsibility of the sender to only send e-mails that have actually been requested by the recipient.

6.4 Case 4: Sending tracked e-mails from Outlook using Eloqua for Microsoft Outlook

Sales person of a European company or resides in Europe, using Eloqua for MS Outlook sends an introduction e-mail from his/her Microsoft Outlook to a prospect to make contact.

Under EU law, it does not make a difference if an unsolicited e-mail is sent in bulk by automated means or if the customer sends individual marketing email communications. Under Directive 2002/58/EC, both forms may be considered as 'unsolicited communication' unless the following steps are taken:

1. The Eloqua customer has obtained the e-mail address with the consent of the recipient or otherwise in accordance with the respective data protection law and

© 2011 Eloqua Corporation. All rights reserved.

2. The recipient may, at any time, request not to receive any further communications. Using a Verify & Send method for your Eloqua for Microsoft email will allow you to send a templated email that contains a Manage Subscriptions footer.

As the prospect/recipient is being automatically tracked in a one-to-one communication scenario, what, if anything, must be in the e-mail?

Tracking of e-mails is only compliant when the European data protection legislation is followed. If the recipient has declared his/her consent then you are able to send tracked emails from Microsoft Outlook. To do this there are two main ways:

1. The best way, is by requesting the recipient to register and in doing so, declare his/her consent.
2. A second and viable alternative is to include information about the tracking at the bottom of the e-mail and provide the recipient with the option to opt-out

Caution!

NOTE: The above two options comply with EU data protection law but are technically not compliant with German data protection law. However, at this time, data protection authorities in Germany **will not** prosecute such practices.

Please consult your company's legal council before proceeding with such practices and procedures.

7.0 Resources

Eloqua's robust technology allows for compliance with all current EU email and privacy regulations. A brief description and links to instructional articles are listed in this section.

7.1 Visitor Tracking Opt Out Instructions

In order to comply with choice requirements in the EU, an option to opt out of website tracking must be made available to all visitors. In most cases, adding a tracking opt out option to the privacy policy will suffice; however in Germany, a visitor must opt in to tracking **before** they are tracked as an **identifiable** visitor. Use the Cookie Opt Out instructions outlined here to implement this option on your website. For the German scenario, you must provide the option to opt in to tracking at the point of collection (i.e. webforms) since that point of collection will link the visitor and any historical visits known via a link to a contact record within the Eloqua database. The best way to achieve this is to use a reverse of the stated option on the tracking option selection page, whereby the opt-out cookie is set if the visitor does **not** check the tracking opt in option on the webform.

© 2011 Eloqua Corporation. All rights reserved.

7.2 Confirmed Opt In Process

While not a legal requirement throughout the EU, a Confirmed Opt In process should be implemented when collecting an email address from anyone you intend to email. This process involves sending a confirmation email to the address that the visitor enters into your webform **before** they are added to Eloqua as a contact. Use the Confirmed Opt In Process instructions outlined here to implement this process.

7.3 Manage Subscriptions

After providing their affirmative consent to receive emails via the Confirmed Opt In process, email recipients must be provided with the option to remove their consent at any time. Use the instructions outlined here to create a subscription management option to be used in your email footers.

7.4 Master Exclude List

In the event that you are requested to remove a domain, certain recipient, or a certain set of contacts from all future mailings, the Master Exclude List is an important and useful option. Since there is no override for the Master Exclude list like there is for a regular Unsubscribe status in the email Batch Wizard, this list provides a safeguard against an accidental send to, or reset of the contact level unsubscribe.

7.5 Form Layout

Unlike the US, which primarily uses an Opt Out methodology (pre-checked box), the EU has adopted an Opt In (unchecked box) requirement, particularly for email and in the case of Germany, identified visitor tracking. When creating a form for EU signups using these instructions, be sure to leave radio buttons and checkboxes **unchecked** where they pertain to email signups and visitor tracking choice.

© 2011 Eloqua Corporation. All rights reserved.