Readiness Check: Website Certification

Information on the scope of EuroPriSe Website Certification and on its high quality requirements

Introduction

This document provides information on the scope of EuroPriSe Website Certification and on the high quality requirements that websites must meet to be awarded the EuroPriSe seal. It allows website owners to find out whether their website is ready for EuroPriSe Website Certification and to identify any gaps between the as-is and the target situation.

Scope

EuroPriSe Website Certification focuses on the interaction between the browser of a visitor of a website and the web server when the visitor browses the publicly available parts of the website. By contrast, it does not cover data protection issues related to website content (e.g., published pictures, videos and textual information about identifiable persons). However, there is one exception to this general rule: It concerns the publication of personal data that evidently violates the law (e.g., publication of defamatory information such as clearly insulting statements). In such a case, no seal will be granted even if all other EuroPriSe requirements are met.

Website certification is to be distinguished from a certification of a web-based service. Specific services that are often provided via websites are, for example, web shops or access restricted sections of websites offering specific information or other services (e.g., web-based email) to users. Other examples would be web-based search engines or cartographic services. Such services may be suitable targets of evaluation for a certification as an IT-based service but go beyond the scope of a website certification.

Applicable Requirements

EuroPriSe high quality requirements for Website Certification are divided into a total of 15 packages. While the first of these packages ("basic package") deals with data protection issues that are relevant for each and every website, the applicability of the remaining packages depends on the technologies and functionalities that a website is equipped with.

In detail, the following packages may be relevant for a certification of a website according to EuroPriSe:

- Basic package
- Web hosting
- Content Delivery Network
- DOM storage
- Flash cookies
- MS Silverlight cookies
- Device fingerprinting
- Web analytics
- Social plugins
- Online Behavioural Advertising
- Forms on a website
- Newsletter
- Website Recommendation
- Children
- International data transfer

Contact/Office - Germany
Sebastian Meissner
Joseph-Schumpeter-Allee 25
53227 Bonn
Phone: +49 228 763 679 30
contact@european-privacy-seal.eu

Contact - Slovakia
Matej Fatkulin
CSA 4
SK-97701 Brezno
Phone: +421 48 28123-80
contact@european-privacy-seal.eu

Contact - United States
Marcus Belke
2888 Loker Avenue East
Carlsbad, CA 92010
Phone: +1 (917) 8315 180
contact@european-privacy-seal.eu

Commercial Register No.:
Bonn HRB 20387
USt-IdNr (VAT ID):
DE292781061
Website:
www.european-privacy-seal.eu

As a first step in the overall readiness check, website owners are required to identify all relevant technologies and functionalities that their website comes with. Having done this, they can then determine all of the above-listed packages that are applicable when it comes to the certification of the website according to EuroPriSe.

Depending on the outcome of the first step, website owners may then continue the readiness check via jumping to the parts of this document that are relevant for them.

NOTE: The final decision about the applicability of the packages listed above is to be made by EuroPriSe Experts and EuroPriSe Certification Authority.

Overview on Core Requirements

Information on the most relevant high quality requirements for EuroPriSe Website Certification is provided below. This is done in a short and brisk but still meaningful style. This chapter is structured according to the packages that were introduced above.

Website owners should study the information about the requirements that apply to their website carefully. If they identify any shortcomings, EuroPriSe strongly advises them to fix these prior to commencing a website certification project with EuroPriSe Experts and the EuroPriSe Certification Authority.

Basic Package (Always applicable!)

1. Logging of Full IP Addresses

In respect to logging of full IP addresses, the following rules apply:

- Logging is permitted under Art. 7(f) of Directive 95/46/EC (***balancing of interests***) if
  - logging is conducted for specific IT security purposes only (e.g., "prevention of DDoS attacks"),
  - the retention period does not exceed three months (recommendation: maximum retention period = 7 days),
  - any retention period that exceeds the recommendation brings real additional benefits in terms of IT security, and
  - the privacy notice informs about all relevant aspects of the logging.
- IP addresses may be logged for a period of time exceeding three months, if the website owner collects website visitors' ***prior consent*** and provided that consent is freely given and informed (Art. 7 (a) of Directive 95/46/EC).

2. Use of HTTP Cookies

EuroPriSe distinguishes between the use of "strictly necessary cookies" and "not strictly necessary cookies." When it comes to the latter ones, EuroPriSe distinguishes further between "session cookies" and "persistent cookies."

Contact/Office - Germany
Sebastian Meissner
Joseph-Schumpeter-Allee 25
53227 Bonn
Phone: +49 228 763 679 30
contact@european-privacy-seal.eu

Contact - Slovakia
Matej Fatkulin
CSA 4
SK-97701 Brezno
Phone: +421 48 28123-80
contact@european-privacy-seal.eu

Contact - United States
Marcus Belke
2888 Loker Avenue East
Carlsbad, CA 92010
Phone: +1 (917) 8315 180
contact@european-privacy-seal.eu

Commercial Register No.:
Bonn HRB 20387
USt-IdNr (VAT ID):
DE292781061
Website:
www.european-privacy-seal.eu

a. "Strictly necessary cookies"

"Strictly necessary cookies" are cookies that are covered by one of the two exceptions of Article 5(3), sentence 2 of the ePrivacy Directive, i.e. cookies that are (1) used for the sole purpose of carrying out the transmission of a communication over an electronic communications network or (2) strictly necessary in order for the provider of an information society service, which was explicitly requested by the user, to provide the service.

In respect to "strictly necessary cookies", the following rules apply:

– EuroPriSe accepts the use of http cookies if

  - the cookies are covered by one of the two exceptions of Article 5(3), sentence 2 of the ePrivacy Directive ***during their entire lifetime***, and
  - the ***privacy notice*** informs about all relevant aspects of the use of these cookies (e.g., name, type, purpose, lifetime, content).

b. "Not strictly necessary" session cookies

In respect to "not strictly necessary" session cookies, the following rules apply:

– EuroPriSe accepts the use of session cookies that are not covered by one of the two exceptions of Article 5(3), sentence 2 of the ePrivacy Directive if

  - information on these cookies is provided to visitors via a "cookie notice" (e.g., a cookie banner) when they enter the website for the 1st time.
  - the "cookie notice" is easily recognizable with all typical kinds of devices (including smartphones and tablets).
  - the "cookie notice" is displayed not only when visitors enter the website via its homepage, but also when they follow a deep link to a subordinated page of the site (e.g., subsequent to a web search).
  - the "cookie notice" is displayed
    i. until the visitor takes some explicit action (e.g., clicks an "OK" button – if any) or
    ii. for a period of at least two minutes, if no explicit action is taken (e.g., if the website comes with a "further browsing" solution).
  - the "cookie notice" provides a hyperlink to more detailed information in the privacy notice or a dedicated cookie policy.
  - the "cookie notice" comes with a user-friendly option for website visitors to consent to the use of the cookies:

Contact/Office - Germany
Sebastian Meissner
Joseph-Schumpeter-Allee 25
53227 Bonn
Phone: +49 228 763 679 30
contact@european-privacy-seal.eu

Contact - Slovakia
Matej Fatkulin
CSA 4
SK-97701 Brezno
Phone: +421 48 28123-80
contact@european-privacy-seal.eu

Contact - United States
Marcus Belke
2888 Loker Avenue East
Carlsbad, CA 92010
Phone: +1 (917) 8315 180
contact@european-privacy-seal.eu

Commercial Register No.:
Bonn HRB 20387
USt-IdNr (VAT ID):
DE292781061
Website:
www.european-privacy-seal.eu

i. **STRONG RECOMMENDATION:** The cookie notice comes with declaration of consent text + with an "OK" or "YES" button and a "NO" button.

ii. **STILL ACCEPTABLE** (provided that ***no persistent cookies*** are used that are not strictly necessary)**:** "Further browsing" solution (i.e., The website visitor is informed that he consents to the use of the cookies when he continues browsing by means of following hyperlinks to other pages of the website.)

- the information that is provided via the "cookie notice," privacy notice and cookie policy meets the requirements of an informed consent.
- the consent is renewed at regular intervals and at least once a year.

c. "Not strictly necessary" persistent cookies

Persistent cookies are cookies that remain on the user's device after the end of a browser session.

In respect to "not strictly necessary" session cookies, the following rules apply:

– EuroPriSe accepts the use of persistent cookies if

- information on these cookies is provided to visitors via a "cookie notice" (e.g., a cookie banner) when they enter the website for the 1st time.
- the "cookie notice" is easily recognizable with all typical kinds of devices (including smartphones and tablets).
- the "cookie notice" is displayed even if the visitor follows a deep link to a subordinated page of the site (e.g., subsequent to a web search).
- the "cookie notice" is displayed until the visitor takes some explicit action (e.g., clicks an "OK" button).
- the "cookie notice" provides a hyperlink to more detailed information in the privacy notice or a dedicated cookie policy.
- the "cookie notice" comes with a user-friendly option for website visitors to consent to the use of the cookies such as a declaration of consent text + an „OK" or „YES" button and a „NO" button (a "further browsing" solution does not meet the requirements for persistent cookies that are not strictly necessary).
- cookies are only placed on website visitors' devices if they already consented to the use of these cookies beforehand.
- the information that is provided via "cookie notice," privacy notice and cookie policy meets the requirements of an informed consent.

Contact/Office - Germany
Sebastian Meissner
Joseph-Schumpeter-Allee 25
53227 Bonn
Phone: +49 228 763 679 30
contact@european-privacy-seal.eu

Contact - Slovakia
Matej Fatkulin
CSA 4
SK-97701 Brezno
Phone: +421 48 28123-80
contact@european-privacy-seal.eu

Contact - United States
Marcus Belke
2888 Loker Avenue East
Carlsbad, CA 92010
Phone: +1 (917) 8315 180
contact@european-privacy-seal.eu

Commercial Register No.:
Bonn HRB 20387
USt-IdNr (VAT ID):
DE292781061
Website:
www.european-privacy-seal.eu

- the consent is renewed at regular intervals and at least once a year.
- the "cookie notice" provides website visitors with a user-friendly option to reject the use of not strictly necessary persistent cookies.
- the decision to reject the use of cookies is respected for a period of at least one year until visitors are asked for their consent again.

3. Imprint, Privacy Notice and Cookie Policy (if any)

– The website must come with an imprint that meets all legal requirements of Article 5 paragraph 1 of Directive 2000/31/EC (**NOTE:** EuroPriSe requires websites to meet these requirements even if they are not subject to the provisions of the E-Commerce-Directive).

– The website must come with a privacy notice that informs website visitors about all relevant data processing when they visit the site.

– Both the imprint and the privacy notice must be easily recognizable and be labelled in a meaningful manner.

– Both the imprint and the privacy notice must be hyperlinked directly on each page of the website in the shape of a "one-click solution."

– Both imprint and privacy notice must be available in all languages that are used on the website.

– If the website comes with a cookie policy, it must provide relevant information on the use of cookies and meet the above-mentioned requirements for imprints and privacy notices that are not related to their content.

4. Web Hosting + Content Delivery Networks (CDN)

a. Basics

– Web hosting companies & CDN providers are subject to similar requirements.

– Website certification focusses on the interaction between web server and website visitors' browsers rather than on technical and organizational measures securing hosting and CDN services.

– For this reason, website certification requires only limited technical checks as outlined below at "e."

b. Controller – processor agreement

– A controller – processor agreement between web hosting company / CDN provider which meets the requirements of Article 17 of Directive 95/46/EC must be in place.

c. Transparency

– The privacy notice must inform about the involvement of the web hosting company / CDN provider as a processor on behalf of the website owner.

d. Technical and organizational measures

– Appropriate technical and organizational measures must be in place at the web hosting company / CDN provider.

e. Technical evaluation methods

– Technical experts must verify that the contractual arrangements between website owner and web hosting company / CDN provider or any annexes to them contain a (brief) description of technical and organizational measures that are to be considered appropriate.

– A review of the contractual arrangements or the annexes hereto by the technical experts is not required if

  • the web hosting company / CDN is in possession of a relevant data protection and/or IT security certification (e.g., ISO 27001),

  • the scope of the certification covers the web hosting / CDN services that are provided on behalf of the website owner, and

  • the certification is up-to-date (i.e., It will remain valid at least until the next EuroPriSe monitoring or re-evaluation).

5. DOM Storage, Flash Cookies, Silverlight Cookies & Device Fingerprinting

a. Principle

– Since DOM storage, Flash cookies, Silverlight cookies and device fingerprinting are subject to Article 5(3) of the ePrivacy Directive, they must meet the same requirements that were already outlined before for http cookies.

– Again, EuroPriSe distinguishes between constellations in which a use of these technologies is "strictly necessary" in the meaning of Article 5(3), sentence 2, and other constellations in which this is not the case.

b. Particularities

– DOM storage, Flash cookies, Silverlight cookies and device fingerprinting must not be used as a tool to restore "traditional" http cookies that were refused or erased by the data subject.

Contact/Office - Germany
Sebastian Meissner
Joseph-Schumpeter-Allee 25
53227 Bonn
Phone: +49 228 763 679 30
contact@european-privacy-seal.eu

Contact - Slovakia
Matej Fatkulin
CSA 4
SK-97701 Brezno
Phone: +421 48 28123-80
contact@european-privacy-seal.eu

Contact - United States
Marcus Belke
2888 Loker Avenue East
Carlsbad, CA 92010
Phone: +1 (917) 8315 180
contact@european-privacy-seal.eu

Commercial Register No.:
Bonn HRB 20387
USt-IdNr (VAT ID):
DE292781061
Website:
www.european-privacy-seal.eu

c. Particularities for Flash (cookies) only

– The privacy notice / cookie policy must inform about IT security risks of Flash technology and point website visitors to the fact that they should update Flash technology as soon as any updates closing security vulnerabilities are available.

d. Particularities for device fingerprinting only

– Device fingerprinting is considered to be an invasive technology. Thus, EuroPriSe applies the most severe requirements not only to persistent, but also to session device fingerprinting that is "not strictly necessary":

- EuroPriSe requires the prior informed consent for the use of session device fingerprinting (i.e., Session device fingerprinting may only be used if a website visitor consented to it beforehand.).
- EuroPriSe does not accept a "further browsing" solution when dealing with session device fingerprinting, but requires the consent to be explicit (e.g., A "Yes" button next to a declaration of consent would meet this requirement.).

6. Web Analytics

a. Web analytics tools that may be exempted from the opt-in requirement of Article 5(3)

– Basics

- In WP 194, the Article 29 WP stated, "Should article 5.3 of the Directive 2002/58/EC be re-visited in the future, the European legislator might appropriately add a third exemption criterion to consent for cookies that are strictly limited to first party anonymized and aggregated statistical purposes."
- The French data protection authority CNIL went one step further and identified two web analytics tools that – according to the CNIL – may be exempted from the consent requirement already today.
- EuroPriSe decided to follow the CNIL's approach for the new website certification. This means that website owners who make use of AT Internet (Xiti) and/or Piwik on their website are exempted from the opt-in requirement provided that the following requirements are met:

  i. Requirements for exception

  – The lifetime of the tracking cookie that is used for the purpose of web analytics does not exceed 12 months (after first visit of the website).

  – Visitors' IP addresses are anonymized by means of cutting (at least) the last two bytes.

  – Technical and organizational measures are in place that ensure that the collected information on website usage is not linked to any other information that relates to the website visitor.

- Tracking of website visitors for the purpose of web analytics is limited to the website at hand, rather than visitors being tracked across several websites.
- Website visitors are provided with a user-friendly option to opt-out from the use of the web analytics tool at any point in time and on all types of devices including smartphones and tablets.
- The privacy notice / cookie policy provides website visitors with all relevant information on the use of the web analytics tool.

b. Web analytics tools are subject to the opt-in requirement of Article 5(3)

- Scope
  - This section covers AT Internet (Xiti) and Piwik if they are not exempted from the opt-in requirement of Article 5(3) due to the fact that they do not meet all requirements that are listed in the previous section. Furthermore, any other web analytics tools must meet the requirements of this section as well.
- Principle
  - Web analytic tools may rely on different types of technology such as http tracking cookies. The requirements of all related ToE packages must be met.

7. Social Plugins

a. Definition

- Social plugins are tools that can be implemented in a website and allow website visitors who are users of social networks such as Facebook or Google+ to interact / communicate with other users by means of (e.g., sharing links, commenting or sharing emotions such as "likes."
- Social plugins are also used by other "social services" such as microblogging services (e.g., Twitter), photo sharing services (e.g., Instagram) and bookmarking services (e.g., Addthis.com).

b. Requirements

- Social plugins disabled by default
  - The website shall only open a communication channel between website visitors and provider of the "social service" after visitors expressed their intention to make use of the social plugin by means of an explicit action.
- Transparency
  - The privacy notice provides meaningful information on the privacy implications of the social plugins that are implemented in the site in the privacy notice.

- The website comes with a hyperlink to the information on social plugins in the privacy notice that is located in close proximity to the interactive icons ("buttons") that allow the user to make use of the social plugins, and the hyperlink is easily recognizable and comes with meaningful information.

– International data transfers

- Since the vast majority of large social service providers is located outside of the European Economic Area, it is to be highlighted that any transfer to a third country outside of the EEA must be covered by a legal justification.
- EuroPriSe provides detailed guidance on what website owners must do in order to rely on an informed consent as legal justification for such an international data transfer in the online evaluation tool.

c. Best practice recommendation

– "Two clicks for more privacy"
www.h-online.com/features/Two-clicks-for-more-privacy-1783256.html

– "Shariff - Give Social Media Buttons Some Privacy" (advancement of two clicks solution)
www.github.com/heiseonline/shariff/blob/master/README.md

8. Online Behavioural Advertising

a. Basics

– In WP 171, p. 11, the Article 29 Working Party considered that while OBA providers are responsible for the requirements of Article 5(3) of the ePrivacy Directive being met, publishers (website owners) have a certain limited responsibility for the data processing that results from the use of an OBA service.

– Based on this initial position, EuroPriSe requires website owners who implemented an OBA service into their websites to meet the requirements listed below.

b. Requirements

– Transparency

- The website comes with an easily recognizable "OBA notice" (e.g., a banner) that provides information on the OBA topic to website visitors as they enter the website (homepage or any sub-pages) for the 1st time.
- The "OBA notice" is displayed
  i. until the visitor takes some explicit action (e.g., clicks an "OK" button – if any) or
  ii. for a period of at least two minutes, if no explicit action is taken (e.g., if the website comes with a "further browsing" solution).

Contact/Office - Germany
Sebastian Meissner
Joseph-Schumpeter-Allee 25
53227 Bonn
Phone: +49 228 763 679 30
contact@european-privacy-seal.eu

Contact - Slovakia
Matej Fatkulin
CSA 4
SK-97701 Brezno
Phone: +421 48 28123-80
contact@european-privacy-seal.eu

Contact - United States
Marcus Belke
2888 Loker Avenue East
Carlsbad, CA 92010
Phone: +1 (917) 8315 180
contact@european-privacy-seal.eu

Commercial Register No.:
Bonn HRB 20387
USt-IdNr (VAT ID):
DE292781061
Website:
www.european-privacy-seal.eu

iii. The "OBA notice" provides basic information on the use of the OBA tool(s) / service(s).

iv. The "OBA notice" provides a hyperlink to more detailed information in the privacy notice / cookie policy.

v. The privacy notice / cookie policy provide all relevant information on the use of OBA tool(s) / services.

– Opt-Out

  • The website must provide visitors with a user-friendly option to opt-out from the use of OBA at any point in time.

9. Forms on the Website

a. Newsletter form

– Cf. below at "10."

b. Contact / feedback form

– Confidentiality

  • Personal data which may be communicated via the contact / feedback form are encrypted by means of proper SSL encryption by default.

– Data minimization

  • When visitors make use of the contact / feedback form, they are not asked to provide any personal data mandatorily that goes beyond the website visitor's name and email address.

– Transparency

  • The website comes with basic information on how personal data that is collected via the contact / feedback form are used and a hyperlink to the relevant section of the privacy notice. This information and the hyperlink are both located in close proximity to the contact / feedback form or, as a minimum, the website comes with a hyperlink to the relevant section of the privacy notice, and the hyperlink is located in close proximity to the contact / feedback form.

  • The privacy notice provides all relevant information on the processing of personal data that results from the use of the contact / feedback form.

c. Any other forms

– Confidentiality

- Personal data that may be communicated via any other form are encrypted by means of proper SSL encryption by default.

– Data minimization

- The website does not collect excessive personal data on a mandatory basis when other types of forms are used. Necessity of data depends on the purpose of the respective form.

– Transparency

- The website comes with basic information on how personal data that is collected via other types of forms are used and a hyperlink to the relevant section of the privacy notice. This information and the hyperlink are both located in close proximity to the respective form or, as a minimum, the website comes with a hyperlink to the relevant section of the privacy notice, and the hyperlink is located in close proximity to the respective form.
- The privacy notice provides all relevant information on the processing of personal data that results from the use of any other types of forms.

10. Newsletter

a. Newsletter subscription form

– Confidentiality

- Personal data that may be communicated via the newsletter subscription form are encrypted by means of proper SSL encryption by default.

– Data minimization

- When visitors make use of the newsletter subscription form, they are not asked to provide any personal data mandatorily that goes beyond the website visitor's email address.

– Transparency

- The website logs any submission of the newsletter subscription form.

b. After use of subscription form

– Double opt-in

- The website sends a confirmation email to the email address that the website visitor indicated in the form.
- The confirmation email comes with a hyperlink that allows the recipient of the email to confirm the subscription of the newsletter.
- The email address is added to the newsletter distribution list only after the confirmation of the subscription.

– Opt-out

- Each edition of the newsletter provides subscribers with a valid address or a hyperlink that allows them to opt-out from the subscription.

– Transparency

- The website comes with a hyperlink to the relevant section of the privacy notice, and this hyperlink is located in close proximity to the newsletter subscription form (minimum requirement), or the website comes with said hyperlink and basic information on the newsletter functionality, and both this information and the hyperlink are located in close proximity to the newsletter subscription form.
- The website provides subscribers of the newsletter access to the data protection terms for the subscription of the newsletter that were valid when they subscribed to it at any point in time.
- Website visitors are provided with all relevant information on the newsletter functionality in the privacy notice.

11. Website Recommendation

a. "Tell-a-friend" functionality

– Definition

- The website visitor may use a web form that is provided on the website to recommend the site. Submission of the form results in sending of an email to a recipient email address that the visitor indicated in the form. Sender of the e-mail is the website owner who will usually also provide some recommendation text that is sent to the recipient.

– "Tell-a-friend" is a deal-breaker

- Due to compliance issues with Article 13 of the ePrivacy Directive, the EuroPriSe seal for websites is not awarded to a website that comes with a "tell-a-friend" functionality as defined above.

- Possible solutions for website owners:
  i. Complete removal of "tell-a-friend" functionality
  ii. Switch from "tell-a-friend" to "mail-to" functionality. (cf. below)

c. "Mail-to" functionality

– Definition

- The website visitor may click on an icon or text. As a result, the visitor's mail client (if embedded) will open and create a new message with some basic recommendation text regarding the website. After entering the recipient's email address and modifying the subject line and / or the recommendation text, the visitor may send the email to the recipient. In contrast to the "tell-a-friend" scenario, the website visitor is the sender of the recommendation email.

– Requirements

- The website does not collect / log any personal data (including IP addresses) in the context of the "mail-to" functionality that goes beyond the logging that was examined by the experts when dealing with the "basic package."
- The recommendation message does not come with a subject line and/or a recommendation text which is overly lengthy and/or overly praising.
- The privacy notice provides all relevant information on the "mail to" functionality.
- **RECOMMENDATION:** Add a link to the relevant section of the privacy notice and place the link in close proximity to the "mail-to" functionality.

12. Children

a. Applicability of children package

– The package is applicable if the website at hand is explicitly addressed to minor visitors. This is not only the case if all website content is addressed to children, but also if some website content is addressed to them (e.g., if a web page of a newspaper comes with a "kids corner").

b. Requirements

– The website does not track website visitors within areas of the website that are dedicated to children.

- **NOTE 1:** Tracking refers to the monitoring of how website visitors make use of the areas of the website that are dedicated to children.

- **NOTE 2:** Since website owners cannot determine if an adult or a kid browses webpages that are dedicated to children, they must refrain from tracking visitors of relevant pages completely in order to meet this requirement.

– The website only does collect personal data about website visitors via functionalities that are explicitly addressed to children with prior parental consent, provided that parental consent is required.

– If parental consent is required: The website makes reasonable efforts to verify that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology.

– The website does not collect excessive personal data on a mandatory basis when website visitors make use of functionalities such as specific forms which are explicitly addressed to children.

– The privacy notice makes use of simple, concise and educational language that can be easily understood when informing children about the processing of their personal data on the website via the privacy notice.

13. International Data Transfers

a. Scope

– Each type of transfer of personal data relating to website visitors from within the EEA to a country outside of the EEA that has been identified by the Technical Expert must be covered when dealing with this package.

b. Requirements

– The website only transfers personal data to third countries outside of the EEA if a proper legal justification is in place (cf. Art. 25 f. of Directive 95/46/EC).

c. Consequences of Schrems judgment of European Court of Justice

– Safe Harbor is not a valid legal justification anymore.

– For the time being, Standard Contractual Clauses and Binding Corporate Rules are still accepted as proper legal justifications for international data transfers by EuroPriSe CA. However, future judgements of the CJEU and future opinions of the Article 29 Working Party may change this. They will have to be considered within a EuroPriSe website certification project as soon as they are applicable.