EuroPriSe
European
Privacy Seal

European Privacy Seal

– privacy at its best

EuroPriSe Criteria

(November 2011)

EuroPriSe Criteria
(November 2011)

www.european-privacy-seal.eu

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98 - 24103 Kiel - Germany
Tel.: +49 431 988 1208
europrise@datenschutzzentrum.de

Content

Introduction

This document lists the **EuroPriSe criteria and requirements** as well as relevant questions relating to them.

The document is divided into two parts. Part 1 addresses preliminary issues: the scope of the European Privacy Seal, crucial EuroPriSe definitions, and the target of evaluation (ToE); whereas part 2 consists of the EuroPriSe Criteria as such, comprising four sets of requirements and criteria.

The EuroPriSe Criteria document is regularly updated. In particular, it is adapted to changes in EU privacy legislation as well as to developments in information technology.

Part 1: Preliminary Issues

A. Scope of the European Privacy Seal

The European Privacy Seal certifies that an IT product or IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection, taking into account the legislation in the EU Member States.

B. Definitions

Data, Primary

Primary data are data that are primarily processed by the IT product or IT-based service (e.g., name of a person, payment data).

Data, Secondary

Secondary Data are data which are incidentally produced when the product or service is used (e.g., usage data, log files, statistical data, data for authorisation, configuration data). These data can be personal data on the data subjects, personal data on the people operating the product or service, or privacy-relevant configuration data.

IT Product

Products suitable for certification are IT products such as hardware (e.g., a hardware firewall) and software (e.g., a database application).

IT-Based Service

Services suitable for certification are IT-based services such as web-based services (e.g., online banking or search engine services) and processing of data by a processor (e.g., a data centre hosting mail servers).

Target of Evaluation (ToE)

The ToE is the concrete subject of an evaluation. The evaluation subject may be a complete product, a part of a product, a composition of several products or a specific substantial technology. The same applies to IT-based services.

C. Target of Evaluation (ToE)

The Target of Evaluation is the concrete object of an evaluation. It may be either one or several part(s) of an IT product, a complete product or even a combination of several products. The same applies to IT-based services. An accurate specification of the target of evaluation (ToE) is of fundamental importance for a certification procedure, as it decides on what is covered by the certification. Even small changes of the ToE may have a serious impact on the evaluation and its results. The ToE is one important part of each evaluation report to be drafted by EuroPriSe Experts. At the beginning of the report, the ToE and its exact area of application have to be determined as accurately as possible. Furthermore, the data flow resulting from the use of the product or service is to be illustrated and the legal provisions applicable for the certification are to be determined.

ToE Analysis

Relevant Questions:

- Does the ToE qualify as an IT product or as an IT-based service?
- What precisely is the Target of Evaluation? Which components of the product or service are parts of it, which are not?
- What types of (personal) data are processed when the product or service is used? Which of these data are primary, which are secondary data?
- What data flows occur when the product or service is used?
- What is the area of application of the product or service?

Regulatory Analysis

Relevant Questions:

- What legal or technical regulations are applicable with regard to the (intended) use of the ToE?

Part 2: EuroPriSe Criteria

The EuroPriSe Criteria consist of the following four sets:

- Set 1: Overview on Fundamental Issues
- Set 2: Legitimacy of Data Processing
- Set 3: Technical-Organisational Measures
- Set 4: Data Subjects' Rights

Set 1: Overview on Fundamental Issues

The first set covers **fundamental issues**. Questions posed in this set aim to provide an overall picture of privacy relevant issues relating to the ToE. The first part of the set concerns fundamental processing aspects such as processing operations, processed data, and pursued purposes, while the second part deals with the fundamental technical construction of a product or service, i.e. with topics such as data avoidance/minimisation and transparency.

1.1 Fundamental Aspects of Processing

1.1.1 Processing Operations; Purpose(s)

(Articles 2(b) and 6(1) (b) of Directive 95/46/EC)

Relevant Questions:

- What different processing operations are associated with the use of the product or service?
- What is the main operation?
- What further purposes are or can be served by the product or service?
- Are all the purposes sufficiently specifically defined?
- To which recipients are data disclosed (in-house and externally)? For what purposes?

1.1.2 Processed Personal Data

(Articles 2(a) and 8 of Directive 95/46/EC)

1.1.2.1 Personal Data

(Article 2(a) of Directive 95/46/EC)

Relevant Questions:

- Are any personal data processed when the product or service is used?
- If yes: Which of the data processed when the product or service is used constitute personal data?

1.1.2.2 Special Categories of Data

(Article 8 of Directive 95/46/EC)

Relevant Questions:

- Are special categories of data processed when the product or service is used?

1.1.3 Controller

(Article 2(d) of Directive 95/46/EC)

Relevant Questions:

- Who is the controller of each processing operation?
  - Will the vendor of the product or the provider of the service remain the controller of some or all of the operations?
  - Or will the buyer or user of the product or service become the controller?
  - Is this clarified in the documentation provided with the product or service?
- Are data processed on behalf of the controller (Article 2(e), 17(2)-(4) of Directive 95/46/EC)?

1.1.4 Transnational Operations

(Article 25 f. of Directive 95/46/EC)

Relevant Questions:

- Are data transferred to countries that are neither a member of the EU nor of the European Economic Area when the product or service is used?

1.2 Fundamental Technical Construction

1.2.1 Data Avoidance and Minimisation

(Articles 6 and 7 of Directive 95/46/EC)

Relevant Questions:

- Is it possible to carry out the processing without the use of identifiable data altogether?
- Are data automatically anonymised or pseudonymised? Or otherwise (e.g., on request)? On what does this, and the timing, depend? How are pseudonymous data secured against too-easy re-identification?
- Are data only collected in identifiable form to the extent strictly necessary in relation to the purpose(s) for which they are collected?
- Which combination of personal data is really necessary? What are the criteria this depends on? To what extent is it really necessary to combine certain data?
- Are measures taken to avoid the unnecessary creation of temporary shadow files (e.g., through unnecessary logging)? If such temporary shadow files are needed, how well are they protected against unauthorised access?
- If data are passed on to other controllers (or processors), are measures taken to filter out data that are not needed by the recipients?

- How long are the data retained? Is this no longer than necessary for the purposes concerned?

1.2.2 Transparency

(Article 6(1) (a) of Directive 95/46/EC)

1.2.2.1 Transparency and Description of the Product or Service

Relevant Questions:

- Is transparency ensured with regard to data processing (data flow, data location, ways of transmission, etc.) in respect of users of the product or service as well as data subjects?
- Is an informative, up-to-date and understandable, well-indexed/searchable description of the product or service provided to the user? Is it simple to access the description? How is this updated?
- Is the basic concept underpinning the product or service clearly set out?
- Is special knowledge needed for understanding the description of the product (language / know-how)?
- Is the source text accessible or the can the hardware be opened? To whom? Also to external parties or only to experts?

1.2.2.2 Special Case: Privacy Statement

In the context of the Internet, information on privacy issues is usually provided via privacy statements. If this is the case, it has to be checked whether there is a privacy statement in place that provides sufficient information about the product or service, in an appropriate manner.

Relevant Questions:

- Is an informative, up-to-date and understandable privacy statement in place?
- Does the privacy statement provide sufficient information on relevant privacy issues (e.g. use of cookies, processing of IP addresses)?
- Does the privacy statement provide specific and meaningful information about the processing of personal data instead of mere blanket confirmations of legal compliance?
- Is the concept of “highlight notices” used (providing some high level information at a glance)?
- Is the privacy statement available in one / multiple language(s)?
- Is the statement prominently linked on the home page of the respective website? Is it linked on all other pages of the website?
- Does the privacy statement inform about the identity of the data controller? Does it provide contact details to enable contacting in case of questions or complaints

Set 2: Legitimacy of Data Processing

Set 2 concerns the **legitimacy of data processing**. In particular, set 2 deals with the question of the legal basis of the processing, special requirements relating to the various phases of the processing, compliance with general data protection principles and –duties, and a number of special types of processing operations.

2.1 Legal Basis for the Processing of Personal Data

2.1.1 Legal Basis for the Processing of Personal Data in General

(Article 7 of Directive 95/46/EC)

2.1.1.1 Processing on the Basis of Consent

(Article 7(a) of Directive 95/46/EC)

Relevant Questions:

- Does the consent (as expressed by the data subject) meet the legal requirements on consent?
  - Is the consent unambiguous and sufficiently specific, by setting out the purpose of the various phases of the processing?
  - Is it obtained under some form of duress / an offer of advantage / threat of disadvantage? Does any of this invalidate the consent?

2.1.1.2 Processing on the Basis of a Contract

(Article 7(b) of Directive 95/46/EC)

Relevant Questions:

- Does the use of the product or service involve only processing of personal data that are strictly needed for the performance of the contract? If not:
  - Does the contract to be signed by the data subject include provisions allowing for the collection of more personal data than strictly needed for the performance of the contract?
  - Are those provisions acceptable?
  - Is it made clear to the user what the purpose is for which additional information is asked, and that the provision of this additional information is voluntary?

2.1.1.3 Processing on the Basis of Legal Obligation

(Article 7(c) of Directive 95/46/EC)

Relevant Questions:

- What legal provision does establish the obligation?
- Does the law (or a regulation under the law) exclusively list the data that are to be / may be collected and further processed? If so, does the product or service ensure compliance with this (e.g. by not providing for “free fields”)?
- If the law does not itself specify what data may be collected: Is the processing / are the data really necessary to meet the obligation?

2.1.1.4 Processing on the Basis of Vital Interests

(Article 7(d) of Directive 95/46/EC)

Relevant Questions:

- What are the relevant vital interests?
- How is “vital” interpreted?
- Is it necessary to rely on this criterion, or can the consent of the data subject be obtained?

2.1.1.5 Processing on the Basis of a Public Task

(Article 7(e) of Directive 95/46/EC)

Relevant Questions:

- What is the relevant legal provision?
- Is the processing / are the data really necessary for that task?

2.1.1.6 Processing on the Basis of Balancing of Interests

(Article 7(f) of Directive 95/46/EC)

Relevant Questions:

- What legitimate interests of the controller are served by the processing?
- What fundamental rights and interests of the data subject are affected by the processing?
- Is the right balance struck between these competing interests (i.e. do the legitimate interest of the controller override the rights and interests of the data subject)?

2.1.2 Legal Basis for the Processing of Sensitive Personal Data

Article 8, par. (2), (4) and (6) of Directive 95/46/EC

2.1.2.1 Processing of Sensitive Data on the Basis of Explicit Consent

(Article 8 (2)(a) of Directive 95/46/EC)

Relevant Questions:

- Does the consent (as it is to be expressed by the data subject) meet the requirements of consent?
- How explicit is the consent?

2.1.2.2 Processing of Sensitive Data in the Field of Employment Law

(Article 8(2)(b) of Directive 95/46/EC)

Relevant Questions:

- To what obligations and specific rights of the controller in the field of employment law does the processing relate?
- How specific is the authorisation in the law? Does it cover the processing?
- What safeguards are provided for in the law? Are these complied with?

2.1.2.3 Processing of Sensitive Data on the Basis of Vital Interests

(Article 8(2)(c) of Directive 95/46/EC)

Relevant Questions:

- What are the relevant vital interests?
- How is “vital” interpreted?
- Is the data subject physically or legally incapable of giving his consent?

2.1.2.4 Processing of Sensitive Data for a Not-For-Profit Body

(Article 8 (2) (d) of Directive 95/46/EC)

Relevant Questions:

- Are personal data processed by a body that has a political, philosophical, and religious or trade union aim? Is this body non-profit seeking?
- Is the processing carried out in the course of the body’s legitimate activities? Who determines this?
- Does the processing indeed relate solely to the members of the body or to persons who have regular contact with it in connection with its purposes?
- Are personal data only disclosed to a third party with the consent of the data subjects?

2.1.2.5 Processing of Published Sensitive Data

(Article 8(2)(e) of Directive 95/46/EC)

Relevant Questions:

- Does the processing relate to data which are manifestly made public by the data subject?
    - When can it be said that certain sensitive information has been manifestly made public by the data subject?
    - What about a person's skin colour, or an obvious physical handicap such as blindness?

2.1.2.6 Processing of Sensitive Data for the Defence of Legal Claims

(Article 8(2) (e) of Directive 95/46/EC)

Relevant Questions:

- Does the processing relate to data which are necessary for the establishment, exercise or defence of legal claims?
    - How is it to be determined whether certain sensitive data are necessary for the establishment, exercise or defence of legal claim?
    - Who determines this?

2.1.2.7 Processing of Sensitive Data on a Special Legal Basis

(Article 8(4) and (6) of Directive 95/46/EC)

Relevant Questions:

- What is the relevant legal basis?
    - What substantial public interest is served by this?
    - Is the processing limited to certain sensitive data and / or certain purposes?
    - What safeguards are imposed on the processing? Are these complied with?
- Has this special legal basis been notified to the European Commission?

2.1.3 Requirements of Data Processing for Certain Special Purposes

Article 8, paras. (3) and (5)-(7) and Article 9 of Directive 95/46/EC

2.1.3.1 Processing of Sensitive Data for Medical and Related Purposes

(Article 8(3) of Directive 95/46/EC)

Relevant Questions:

- Are sensitive data collected for any of the following purposes: preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services? If so:
  - Are the data required for that purpose, and are no more data collected than are required for that purpose?
  - Are data anonymised or pseudonymised whenever possible, in particular for use for such secondary purposes?
  - Are the data processed only by health professionals? Are they subject to professional secrecy? Under what law or rules?
  - If the data are processed by people who are not health professionals, are they subject to an equivalent obligation of secrecy? Under what law or rules?

2.1.3.2 Processing of Data on Criminal Convictions

(Article 8, paras. (5) and (6) of Directive 95/46/EC)

Relevant Questions:

- Are data collected that relate to criminal offences, criminal convictions or security measures? If so:
  - Are the data processed only under control of official authorities? Under what law?
  - Are the data processed by non-official bodies? If so:
    - Under what law?
    - What safeguards are set out in those laws? Are they suitable and sufficiently precise?
    - Do they stipulate and ensure that the data do not turn into a complete record of criminal convictions?
  - Has this special permission to process such data been notified to the European Commission?

2.1.3.3 Processing of Data on Administrative Sanctions and Civil Judgments

(Article 8, paras. (5) and (6) of Directive 95/46/EC)

Relevant Questions:

- Are data collected that relate to administrative sanctions and/or judgements in civil cases? If so:
  - Does the national law of the EU Member States specify that these data may be processed only under the control of official authorities? Under what law?

- Does this law lay down conditions on the processing of such data, even by official authorities?
- Has this special permission to process such data been notified to the European Commission?

2.1.3.4 Processing of National Identification Numbers and other General Identifiers

(Article 8(7) of Directive 95/46/EC)

Relevant Questions:

- Does the applicable national law impose restrictions or formalities on the use of the number in question?
- Are these restrictions or formalities complied with / is the user of the product or service alerted to the need to comply with these restrictions or formalities?

2.1.3.5 Processing of Data for the Sole Purposes of Journalism or Artistic or Literary Expression

(Article 9 of Directive 95/46/EC)

Relevant Questions:

- Is the product or service aimed at (or linked to) processing for journalistic, artistic or literary expression? If so:
  - Is this the sole purpose? Who determines this and how?
  - Does the applicable national law contain any special regulations for the processing of data for those purposes?

2.1.4 Special Restrictions on Certain Data Processing under Directive 2002/58/EC

Directive 2002/58/EC contains special provisions on the processing of traffic and location data generated in the context of the provision of electronic communication services, as well as on the making of unsolicited direct marketing contacts to users and subscribers by means of such communications. If this Directive is applicable, these provisions have to be considered.

2.1.4.1 Special Restrictions on the Use of Cookies and other Information Stored in the Terminal Equipment of a Subscriber or User

(Article 5(3) of Directive 2002/58/EC)

Relevant Questions:

- Does the product or service involve the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user?
- Is ensured that information is only stored or accessed if the subscriber or user concerned has given his or her consent?

- How is the subscriber or user concerned asked for his or her consent? Does this ensure that he or she freely gives a clear, unambiguous and specific indication of his or her wishes?
- Has the subscriber been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing?

- If not:
  - Is the sole purpose of the technical storage or access to carry out the transmission of a communication over an electronic communications network?

  or

  - Is the technical storage or access strictly necessary in order to provide an information society service explicitly requested by the subscriber or user?

2.1.4.2 Special Restrictions on the Processing of Traffic Data

(Article 6 of Directive 2002/58/EC)

Relevant Questions:

- Does the product or service involve the processing of traffic data? If so:
  - For what purpose(s)? Does this include marketing or the provision of value-added services? If so:
    - Has the subscriber consented to this? Or the user? On the basis of what information? When was this information provided (cf. Art. 6(4) of Directive 2002/58/EC)? In what form is such consent given? How is it recorded? How can the subscriber withdraw his or her consent? How and when is this given effect?
  - How long are the data retained (other than for the benefit of law enforcement under Directive 2006/24/EC)? Are the data erased as soon as possible? In particular, are traffic data automatically erased immediately after the communication if they are not needed for the purposes of subscriber billing and interconnection payments (as in flat-rate fee arrangements)?
  - Are (copies of) the data retained for the benefit of law enforcement under Directive 2006/24/EC? If so, what measures are taken to ensure that those data are completely separated from the original data? What are the internal procedures to be followed when the authorities demand access to those data? Are logs kept? Are the data subjects informed? Who decides this?

2.1.4.3 Special Restrictions on the Processing of Location Data

(Article 9 of Directive 2002/58/EC)

Relevant Questions:

- Does the product or service involve the use of location data? If so, for what purpose(s) / for the provision of what kind of service?
- Are the data that are passed on to the (value-added) service provider limited to what is strictly necessary for the provision of the service?
- Has the subscriber consented to (or specifically requested) this service? How is this done and recorded? How can the subscriber withdraw his or her consent?
- Can the subscriber temporarily disable this function? Does this really mean that no location data are recorded, at all?
- Are (copies of) the location data retained for the benefit of law enforcement under Directive 2006/24/EC)? If so, answer the questions in this respect that were put under the previous heading.

2.1.4.4 Special Restrictions on the Making of Unsolicited Direct Marketing Contacts with Subscribers

(Article 13 of Directive 2002/58/EC)

Relevant Questions:

- Does the product or service relate to the sending of commercial (direct marketing) messages? If so:
  - Does it relate to “relationship marketing” (marketing directed at the company’s own customers)? Or to marketing to others / the general public?
  - What kinds of means of communication does it involve? Depending on this:
  - Does it require prior consent before the sending of such messages? (“opt-in”)
  - Is an “opt-out” offered?
  - How can the data subject express his or her preferences? Through a national “preference scheme” or (also / only) through direct communication with the company?
  - What measures are taken to ensure that this choice is complied with? How effective are these measures?
  - What records are kept in this regard?
  - If the means of communication is electronic mail:
    - Is ensured that the identity of the sender on whose behalf the communication is made is neither disguised nor concealed, but clearly indicated to recipients of the commercial message?
    - Is ensured that the sending of commercial electronic mail does not contravene Article 6 of Directive 2000/31/EC?

- Is ensured that the recipient may send a request to a valid address that such communications will stop?
- Is ensured that recipients are not encouraged to visit websites that contravene Article 6 of Directive 2000/31/EC?

2.2 Special Requirements to the Various Phases of the Processing

This subset deals with special requirements relating to the different phases of processing of personal data (e.g., information duties of the controller when he or she is collecting data or the duty to erase data when they are no longer needed).

2.2.1 Data Collection (Information Duties)

(Article 10 and 11 of Directive 95/46/EC)

Relevant Questions:

- Are data collected from the data subject or from other sources?
- If data are collected from the data subject: Are data secretly recorded (unknown to the data subject) as, e.g. in certain biometric applications?
- Are the sources of the data recorded?
- Are the data subjects and relevant third parties informed of various matters, as required by law?

2.2.2 Internal Data Disclosure

(Article 6, paras. (b) and (c), Articles 7, 10 and 11 of Directive 95/46/EC)

Relevant Questions:

- Are data internally disclosed only to those who need access? How is this ensured?
- Are the data disclosed internally for a different purpose than the purpose(s) for which the data were originally obtained? If so:
    - What is the legal basis for the disclosure and further processing?
    - Are the secondary purposes in question compatible with the primary purpose for which the data were originally collected?
    - Are only those data disclosed that are needed by the recipients for such further processing / the relevant secondary purposes?
    - Were the data subjects informed of this, either when the data were obtained from them or no later than at the time of the first disclosure for this new purpose? Or did they already have this information? If so, how did they acquire this information?

2.2.3 Disclosure of Data to Third Parties

(Article 6, paras. (b) and (c), Articles 7, 10, 11 and 14(b) and 17(1) of Directive 95/46/EC)

Relevant Questions:

- Are the data passed on to any third parties for the original purpose for which the data were collected? If so, who are these third parties? Was the data subject informed of the intended disclosures, of the specific data or at least of the categories of data that are disclosed, and of the identity of the third party recipients, or at least of the category of third party recipients?
- Are disclosures to third parties recorded / logged? If this is required by law or regulation, is the recording or logging carried out in accordance with the requirements laid down in the relevant law or regulation?
- Are third party recipients informed that they should only use the data for the purpose(s) for which they are provided? Are they asked to warrant that they will do so? Are such warranties binding? Can they be invoked by the data subjects?
- Are only data passed on that are needed for the purpose(s) for which they are to be processed by the third party recipient?
- Are the recipients addresses (e-mail) verified? Are there filters to ensure that the data are not sent to certain recipients/outsiders generally, e.g. by blocking certain (internal or external), or all external email addresses from an organisation's email system?

2.2.4 Erasure of Data after Cessation of Requirement

(Article 6(1) (e) of Directive 95/46/EC)

Relevant Questions:

- Is there a guarantee that all personal data, the actual data used and any back-ups, are erased or de-identified (really anonymised) when they are no longer needed for the purpose for which they were held? How is this done and verified?
- Are specific retention periods set, or moments specified when the data are reviewed? How is compliance with these requirements ensured?
- Can data that are no longer needed for the original purpose, but that cannot be erased due to retention rules (e.g., documentary reasons, tax regulations, etc.), be blocked or otherwise excluded from regular processing?

2.3 Compliance with General Data Protection Principles and –duties

This subset deals with issues arising from general data protection principles and – duties such as purpose-specification and –limitation or quality of data.

2.3.1 Purpose-specification and –limitation

(Article 6(1)(b) of Directive 95/46/EC)

Relevant Questions:

- Are data collected for specified, explicit and legitimate purposes? What are those?
- How is (are) the purpose(s) for which the data are obtained documented?
- Are the data further processed for different purposes than the purpose(s) for which they were originally obtained?
- Are these different purposes compatible with the purpose(s) for which the data were originally obtained?
- Is the processing recorded / logged so as to be able to identify misuse of the data? Is the recording/log tamper-proof?
- Is there data-minimisation, and / or are there measures to prevent the linking of distinct data sets, or to at least make such linking difficult?
- Are data held for certain purposes clearly marked as being held for those purposes, with corresponding access rights, so as to prevent misuse or unauthorised access or disclosure, or to at least make those more difficult?

2.3.2 Proportionality

(Article 6(1)(c) of Directive 95/46/EC)

Relevant Question:

- Assuming that the product or service to be evaluated is used as intended, are the personal data being processed relevant and not excessive in relation to the purposes for which they are collected and/or further processed?

2.3.3 Quality of Data

(Article 6(d) of Directive 95/46/EC)

Relevant Question:

- Are reasonable steps taken to ensure the accurateness, completeness and up-to-dateness of the data?

2.4 Special Types of Processing Operations

2.4.1 Processing of Data by a Processor

(Article 17, paras. (2), (3) and (4) of Directive 95/46/EC)

Relevant Questions:

- Are any data passed to a processor for processing? If so, exactly what data?
- Is this a separate commercial electronic data processing agency or other?
- Is the processing by a processor legally allowed?
- Is the processing by the processor governed by a written contract or other written legal instrument?
- Does this contract or legal instrument stipulate that the processor shall act only as instructed by the controller?
- Does this contract or legal instrument require the processor to adopt all the necessary security measures?
- How does the controller verify compliance with the stipulations in this contract or legal instrument by the processor?
- What guarantees are there to ensure compliance with the legal requirement that the controller shall only process the data on the instructions of the controller, and only as instructed by the controller.

2.4.2 Transfer to Third Countries

(Article 25 f. of Directive 95/46/EC)

Relevant Questions:

- Are data transferred to countries that are neither a member of the EU nor of the European Economic Area (so-called third countries) when the product or service is used?
- Does the third country in question ensure an adequate level of protection? If the third country does not guarantee an adequate level of protection: Is one of the derogations listed in Article 26 of Directive95/46/EC applicable? In particular:
    - Is the transfer necessary for the **performance of a contract** between the data subject and the controller?
    - Is a set of **standard contractual clauses** used that has been approved by the European Commission?
    - Are there **binding corporate rules** in place to ensure compliance, by all those involved, with the requirements of the laws of all EU Member States in which the controller uses equipment to collect and/or further process the data? Have these rules been approved by relevant DPAs?
    - If personal data are transferred to the U.S.: Has the recipient joined the **Safe Harbor** system?

2.4.3 Automated Individual Decisions

(Article 15 of Directive 95/46/EC)

Relevant Questions:

- Does the use of the product or service involve individual decisions that are solely based on automated processing of data? If so:
  - Are the decisions intended to evaluate certain personal aspects relating data subjects concerned, such as their performance at work, creditworthiness, reliability, conduct, etc.? and
  - Do the decisions produce legal effects concerning data subjects or do they significantly affect them?

    If so:
    - Are the decisions taken in the course of the entering into or the performance of a contract? If so: Has the request for the entering into or the performance of the contract, lodged by the data subjects, been satisfied or are there suitable measures to safeguard their legitimate interests, such as arrangements allowing them to put their point of view? or
    - Are the decisions authorised by a law which also lays down measures to safeguard the data subjects' legitimate interests?

2.5 Formalities

2.5.1 Notification

(Article 18(1) and 19 of Directive 95/46/EC)

Relevant Questions:

- Is the processing subject to a requirement of notification (registration)?
  - If so:
    - If the notification is to be done by the user of the product or service: Is the information to be notified readily available (does the product facilitate the easy extraction, provision and up-dating of this information)?
    - If the notification is to be done by the manufacturer of the product or (more likely) the provider of the service: Has the processing in fact been notified?
    - Are procedures in place to ensure that the notification details are updated when necessary?

- If not:
  - Is the processing exempted from the requirement of notification due to the fact that the national law applicable provides for an exemption, where the controller appoints a personal data protection official?

    If so:
    - Has the controller in fact appointed a personal data protection official?
    - Have all relevant information on the processing operations in fact been added to the register of processing operations?
    - May this register in fact be inspected by any person?

2.5.2 Prior Checking

(Article 20 of Directive 95/46/EC)

Relevant Questions:

- Is the processing subject to a prior check? If so:
  - Is the information required for such a check readily available, and made available to the authority or person carrying out the check (does the product facilitate the easy extraction, provision and up-dating of this information)?
  - By whom is this check to be carried out (specifically: by the national DPA or by a controller-appointed data protection official)?
  - Has the processing in fact been checked as required, and found to be compliant with the law?

Set 3: Technical-Organisational Measures: Accompanying Measures for Protection of the Data Subject

Set 3 deals with **technical-organisational measures** aimed at ensuring that the legal requirements are met.

3.1 General Duties

3.1.1 Preventing Unauthorised Access to Data, Programs, Premises and Devices

(Article 17(1) of Directive 95/46/EC)

The prevention of unauthorised access to data is one of the key security measures to prevent loss of integrity, confidentiality and availability of personal data. Access has to be regulated on a physical level and on a logical level: Physical access refers to access to facilities, rooms, hardware, communication line, data media etc., whereas logical access refers to a non-physical access to data, software, functionalities, etc. From a technological point of view, access is not only restricted to access of natural persons, but includes also access of hardware (e.g. access controls of network components such as routers) and software (e.g. access of database drivers to databases).

3.1.1.1 Physical Access Control

Physical access control is relevant for “real life” - the processing of data, for the actual use of IT products and for IT-based services.
Pieces of hardware or software that are subject of a product evaluation will be sold to customers later – it is their duty to implement controls on physical access. Therefore, only IT-based services can be evaluated with respect to the implementation of access control measures.

Relevant for:

- Products:
  - Typically not relevant, if the site of product use is not part of the ToE
  - Sites of product development, manufacturing and delivery, if carried out online (optional)
- Services: Sites of operation (mandatory)

Relevant Questions:

Regarding an IT-based service and sites of product development:

- Which measures prevent unauthorised access to facilities, rooms, hardware, archives, removable media, print-outs etc.?
- Are these measures adequate?

- Are measures used to track accesses? If yes: Apply Section 3.1.2 to the generated data (log data).

3.1.1.2 Access to Media and Mobile Devices

Access control to removable media that store data (tapes, CDs/DVDs, USB-Sticks, removable hard disks, etc.) is crucial because logical access controls (such as write/read rights of files or data base tables, see Section 3.1.1.3) are circumvented once one has access to these media. The same holds for mobile devices storing personal data.

Relevant for:

- Products:
  - Mobile storage of personal data using the product (mandatory)
  - Removable media used in the product's development, manufacturing and delivery (optional)
- Services: use of mobile media in service's operation (mandatory)

Relevant Questions:

Product:

- If the product is a software, and it is possible to use it together with removable media: Information for the user regarding removable media suggested (optional)
- If personal data are stored inside the product in a removable way (e.g., on, SIM-cards etc.) or if the product itself is removable (e.g., handheld devices):
  - Are customers/users informed about these facts and appropriate counter-measures?
  - Are authentication/encryption mechanisms provided?

Service:

- Does the use of service entail (or may it entail) the storing of data on removable media? If so: Are removable media securely stored (e.g., in access restricted archives?) Are print-outs securely stored as well?
- Are media, their content and transmission of media recorded?

3.1.1.3 Access to Data, Programs and Devices

Access to Data and Programs is often controlled by logical means rather than physical means: Typical access control mechanism are rights granted for reading and writing of files or using software or software functionalities, implemented by the operation systems, database management systems or applications. It is to be evaluated if the granularity of access rights is sufficient, having in mind that such systems have to be easy to manage. Furthermore, also the quality of the implementation of access control has to be evaluated, especially in web based applications.

Access to Devices can either be controlled on a logical level (e.g. BIOS passwords, PIN-Codes on telephones or mobile phones) or on a physical level (e.g. electromechanical locks).

Relevant for:

- Products:
  - Processing of personal data using the product (mandatory)
  - Access to personal data, code and sources in product's development, manufacturing and delivery, if carried out online (optional)
- Services: Processing personal data in service's operation (mandatory)

Relevant Questions:

Product:

- Hardware/device: Does the product offer access control facilities (e.g., mechanical locks, PIN code, and password protection)?
- Software: Does the product offer access control facilities, such as a role model?
- Granularity: Can access rights be granted with sufficient granularity, both with respect to the rights (read, altering, transmitting, printing, etc.) and to the data (file, data set, field, table, etc.)?
- Are there specific roles for the administration of access rights (e.g., for granting/revoking of rights, building groups and roles, configuring of roles with respect to user accounts)?
- Can the administration of access rights be separated, e.g. by delegation, from technical administration (e.g. creating back-ups, programming, 2nd-level support, etc.)?
- Is access controlled in every step of the processing, especially in web applications?
- Are countermeasures in place preventing users to manipulate data, esp. measures preventing SQL injections? Have they been tested?
- Are countermeasures in place validating user inputs, esp. measures preventing XSS? Have they been tested?

Service:

- Are access control facilities of products properly used?
- Which persons/roles manage access rights?
- If the service includes the offering of a specific product (e.g., web interfaces as with social networks, online banking, etc. or specific hardware items as locked boxes), the item regarding products have to be evaluated as well.

3.1.1.4 Identification and Authentication

In order to authorise access, users (and also hardware and software) have to be identified and authenticated. Typical mechanisms are login names and passwords, biometrics, security tokens, cryptographic keys (certificates); randomly generated identifiers (e.g., session keys for web applications) are also used for identification and authentication.

Relevant for:

- Products:
  - Processing of personal data using the product (mandatory)
  - Access to personal data, code and sources in product's development, manufacturing and delivery, if carried out online (optional)
- Services: Processing personal data in service's operation (mandatory)

Relevant Questions:

Product and service:

- Does the product/service provide adequate identification and authentication measures? See also Section 3.1.1.5 for authentication based on passwords.
- Does the product/service prevent repeating attempts to identify and authenticate after a certain number of unsuccessful attempts?
- Is the method of prevention (e.g. slowing down identification processes, temporarily deactivation of user accounts, permanent deactivation of user accounts) appropriate?
- If identification and authentication is based on token (e.g., cards, keys, certificates): Are they secured against cloning and unauthorized access?

3.1.1.5 Use of Passwords

If passwords are used for user (or machine) authentication, specific security issues have to be considered. These include, in particular, management, alteration and revocation of passwords. The choice of password complexity, password change mechanisms and storage security has to be adequately in the circumstances.

Relevant for:

- Products:
  - Processing of personal data using the product (mandatory)
  - Access to personal data, code and sources in product's development, manufacturing and delivery, if carried out online (optional)
- Services: Processing personal data in service's operation (mandatory)

Relevant Questions:

Product:

- Which mechanisms ensure that the passwords are assigned, distributed and stored in a confidential and integer way?
- Are they stored in a way that they can not be reconstructed from the stored data, e.g. as hash values?
- Can users easily change passwords?
- Does the product provide mechanisms enforcing password changes in regular intervals?
- Does the product provide mechanisms ensuring appropriate password quality (e.g., length, complexity)?
- Can both, change intervals and quality measures, be configured by administration personnel?
- What happens in the case of forgotten passwords (e.g., issue of a new password? Are forgotten passwords transmitted via email)?

Service:

- Which processes ensure that the passwords are assigned, distributed and stored in a confidential way and retain their integrity?
- Are password changes required at regular intervals?
- Can passwords used for non-human authentication (e.g. authentication codes for WLAN hardware, database access of web servers, etc.) be changed?
- Is a minimum quality of passwords (e.g., length, complexity) required?
- Are support mechanisms of software (e.g., the Operating System) for checking password quality and password lifetime used?
- What happens in the case of forgotten passwords (e.g., issue of a new password? Are forgotten passwords transmitted via email)?

3.1.1.6 Organisation and Documentation of Access Control

Access control has to be managed. This includes the decision on and the documentation of access rights as well as the technical implementation and configuration of access controls. This refers to all kinds of access controls (physical and logical) and also to cases where the management of access rights and of authentication methods are difficult to separate (as in the case of mechanical keys, where access rights can only be revoked by confiscation keys).

Relevant for:

- Products:
  - Processing of personal data using the product (mandatory)
  - Access to personal data, code and sources in product's development, manufacturing and delivery, if carried out online (optional)

- Services: Processing personal data in service's operation (mandatory)

Relevant Questions:

Product:

- Does the product provide mechanisms for easy access to an inventory of granted access rights?
- Are details available about time and person/role granting/revoking access rights?
- Is a history log available? Is this created automatically?

Service:

- Are access rights properly organised, clearly documented, and clear for every authorised user?
- Are rules for access rights administration properly set up and documented?
- Are access rights revoked if they are no longer necessary?
- Are tokens which are used for authentication (such as keys, smart cards, security hardware tokens, etc.) also part of inventories?

3.1.2 Logging of Processing Personal Data

Logging of access to personal data and of their processing is an important measure to ensure the ability to audit processing. Logging files and log data usually contain personal data both on the data subjects (whose data are processed for primary purposes) and on those processing the data (e.g., on employees, but also on the data subjects themselves, in the case of self-service). Therefore, such files are subject to data protection regulations.

3.1.2.1 Logging Mechanisms

The evaluation has to include the question whether sufficient logging mechanisms are implemented.

Relevant for:

- Products:
  - Capabilities of logging mechanisms (mandatory)
  - Capabilities and application of logging mechanisms during product development, manufacturing and delivery, if carried out online (optional)
- Services: Application of logging mechanisms during processing of personal data (mandatory)

Relevant Questions:

Product and service:

- Does the product/service provide logging mechanism aimed at revising/amending/correcting personal data that are being processed? This includes the ability to trace any reading, storing, modification or transmission of such data, as well as the ability to record the identity of the user and the time such actions took place.
- Can/is the logging be configured with respect to the degree of details (e.g., only logging of writing or inserting data, if appropriate)?
- Can/is the retention period for log data be configured?
- Are different types of protocol data (e.g., on the operation of personal data, of transmissions, on the granting of access rights) stored in a way that allows different retention periods (e.g., 2 years for accesses to personal data, 5 years for granting access rights), or are they stored in different log files?
- Does the product/service allow the supplementing of logging data by user input (e.g., input of file numbers to justify data access?)
- Can log data be easily analysed with respect to defined issues (e.g., all modifications of file XXX, all file access between 11 p.m. and 3 a.m., all transmissions made or arranged by user YYY?)
- If logging functionalities are not (or cannot) be provided technically in a service: Are sufficient manual logging mechanisms implemented (e.g., paper-based mechanisms)? For products: Is sufficient information given in the manual in case the product does not support automated logging sufficiently?

3.1.2.2 Operation of Logging Mechanism

Since log data have to be treated as personal data, the evaluation must include the question whether the processing of log data is secured by technical and organisational measures.

Relevant for:

- Products:
  - Operation of logging (mandatory)
  - Operation of logging during product development, manufacturing and delivery, if carried out online (optional)
- Services: Operation of logging during processing of personal data (mandatory)

Relevant Questions:

Product:

- Are the security measures for storage and operation of log data the same as for personal data (e.g. encrypted storage if that is what is done to the other personal data, same back-up cycles)?

- Can reading access rights to log data be granted to non-administrators (e.g. to security or privacy officers)?
- Can the retention period of log data be configured?
- Can logging be blocked/switched off? By whom? Is this logged?

Service:

- Is the retention period configured in accordance with security policies and national legislation? Whose security policies? How are they adopted? What legislation?
- Are logging data periodically reviewed by privacy officers or security officers? (see also Section 3.1.5.7)
- Are log data securely disposed off/(really) destroyed after the retention period?
- Can logging be blocked/switched off? By whom? Is this logged?

3.1.3 Network and Transport Security

Network and transport security refers to the security of IT infrastructure and to the security of transmitted or transported data. Whereas the first aspect usually focuses on the whole infrastructure, the second aspect might be subject to regulations specific to the type of transmitted data, the recipient, etc.

Relevant for:

- Products:
  - Mechanisms for transport of personal data in the product (mandatory)
  - Mechanisms for transport of protection worthy data used during product development, manufacturing and delivery, if carried out online (optional)
- Services: Mechanisms for transport of personal data during processing of personal data (mandatory)

Relevant Questions:

Product:

- Is the security of remote access to the product (software/hardware) comparable to internal access? (Typical measures to ensure this are encryption, VPN, etc.)
- Is the identity of recipients verified (e.g. by certificates), esp. for pull-services?
- Is the transmission of (at least) authorisation data (e.g. username/passwords) secured? The encryption of all transmitted data is strongly recommended, especially for web based services. Does the product support this?
- Is it necessary/appropriate to secure also transmitted content, e.g. with web services (especially for online banking, web mail interfaces, etc.)

Service:

- Is the security of remote access to data or corporate networks comparable to internal access? (typical measures to ensure this are encryption, VPN, two-way authentication, two-factor-authentication etc.)
- Are transmissions over public networks (e.g. Internet) encrypted?
- If there is any connection between internal network and external network: Is the internal network shielded from external or public network, e.g. by firewalls? If yes: Do the firewall rules separate the networks sufficiently?
- Are parts of the network that are accessible both internally and externally (e.g. proxies, mail-Server, etc.) specifically shielded (e.g., places in a DMZ)?
- Is the internal network secured against malware (e.g., transmitted via external links to the network or by attaching mobile devices)?

3.1.4 Mechanisms to Prevent Accidental Loss of Data; Back-up Mechanisms and Recovery

Next to integrity and confidentiality of personal data, availability is also an important objective. Availability is not restricted to data, but covers also the availability of services (including hardware, software and personal aspects). A standard measure is the creation of back-ups, which has to be supplemented by appropriate storage and organisational measures (e.g. recovery tests). Other measures, especially for business- or service-critical data (e.g., health care date) are hardware redundancy (e.g., cold stand-by, hot stand-by) data mirroring (e.g., RAID systems, data replication), or even redundant data centres. Especially for services, whole processes (including data, hardware, but also personal skills and knowledge etc.) have to be backed up in order to minimise infringements due to failures or losses.

3.1.4.1 General Measures

Relevant for:

- Products:
  - General measures implemented in the product (mandatory)
  - Measures used during product development, manufacturing and delivery, if carried out online (optional)
- Services: Measures in place for processing of personal data (mandatory)

Relevant Questions:

Product:

- Are adequate access control mechanisms used to prevent unauthorised erasure or manipulation of data or programs (see Section 3.1.1.3)?
- Are adequate access control mechanisms used to prevent unauthorised disruption of power or network lines or unauthorised deactivation of IT systems (see Section 3.1.1.1)?

- Does the product provide for built in redundancy, or does the manual offer advice for redundant operation of the product? (optional)

Service:

- What measures are taken to protect against fire, water, strong electromagnetic fields, etc.?
- What measures are taken to protect against loss of power?
- Is an availability/redundancy concept available? (optional or mandatory[1]))
- Is a service continuity plan available? (optional)

3.1.4.2 Back-up Mechanisms

Relevant for:

- Products:
  - Mechanisms implemented in the product (mandatory)
  - Mechanisms used during product development, manufacturing and delivery, if carried out online (optional)
- Services: Mechanisms implemented during processing of personal data (mandatory)

Relevant Questions:

Product:

- Does the product offer automated back-up mechanisms?
- Can back-up frequencies be configured?
- Does the back-up include configuration data (e.g. access control data)?
- Can back-ups created by authorised personal only?
- Are back-up data encrypted?
- Does the product provide means for testing the proper working of back-up procedures (e.g., verification of correctness/readability of back-up copies)?
- Is archiving of personal data processed using the product sufficiently discriminated from backing up data?

[1] The decision whether the existence of an availability/redundancy concept is optional or mandatory depends on the concrete circumstances of each individual case.

Service:

- How does the service deal with deletions of data on back-up files?
- Are back-ups performed with the appropriate frequency laid down by national regulations or internal security regulations? (specify the relevant rules and regulations)
- Does the service provide means for testing the proper working of back-up procedures (e.g., verification of correctness/readability of back-up copies)?
- Is archiving sufficiently discriminated from backing up data?

3.1.4.3 Back-up Storage

Relevant for:

- Products:
  - Implementations offered by the product (mandatory)
  - Implementations used during product development, manufacturing and delivery, if carried out online (optional)
- Services: Implementations used during processing of personal data (mandatory)

Relevant Questions:

Product:

- Does the product offer different storage facilities for back-up data (server based, external media, or network?)
- Are back-up data secured against unauthorised access (e.g., through encryption)?

Service:

- Are back-up files stored safely (e.g., in fire-proof safes, at different buildings or locations)?
- Are back-up files secured against unauthorised access (e.g., by encryption, safe, locks)?

3.1.4.4 Recovery

Relevant for:

- Products:
  - Implementations offered by the product (mandatory)
  - Implementations used during product development, manufacturing and delivery, if carried out online (optional)
- Services: Implementations used during processing of personal data (mandatory)

Relevant Questions:

Product:

- Has the product a recovery functionality to recover data from back-ups without re-installation of programs?
- Has the product a recovery functionality to recover configuration data from back-ups without re-installation of programs?

Service:

- Have the recovery processes been tested?
- Is the recovery of single sets of data (e.g., data deleted by mistake) from back-up media organised properly (e.g., only by written authorisation) and documented/logged?
- Is the recovery of single data (e.g., data deleted by mistake) from backup media organised properly (e.g., only by written authorisation) and documented?

3.1.5 Data Protection and Security Management

(Article 4(1a) of Directive 2002/22/EC)

To ensure sustainability of data protection measures, they have to be embedded in a management system. Important aspects of data protection and security measures are: Policy issues, choice and justification of measures, detailed documentation and checks of measures. Additionally, specific measures are regulated in a number of national legislations, e.g., instruction of employees or their obligation to confidentiality.

The majority of management issues are relevant for IT services, but often products will also contribute to management issues, e.g., by providing proper documentation, management functionalities, audit functionalities etc.

3.1.5.1 Security Policy

A security policy is a high level document specifying the overall security objectives, containing the management's commitment to reach these objectives.

Relevant for:

- Products:
  - For products typically not relevant.
  - Policies used during product development, manufacturing and delivery (optional)
- Services: Policies used during processing of personal data (mandatory)

Relevant Questions:

Service:

- Is a written security policy provided or available?
- Are the security objectives effectively pursued by the management?

3.1.5.2 Risk Analysis

Technical and organisational data protection measures have to be chosen with respect to the risk of the infringement of data protection regulations (cf. Article 17 (1) of Directive 95/46/EC). This requires an assessment of "the nature of the data to be protected" (Art. 17 (1)). Some national regulations use a classification scheme (e.g. basic, medium and high) for data and prescribe detailed technical and organisation measures according to this classification.

Relevant for:

- Products:
  - For products (mandatory)
  - For procedures of product development, manufacturing and delivery (optional)
- Services: (mandatory)

Relevant Questions:

Product:

- Does the product documentation provide information on risks, vulnerabilities, etc?
- Does the product documentation provide information on the nature of the data that are being processed, allowing a sufficiently clear classification of data to allow adoption of the appropriate security measures to be taken by the user?

Product development:

- Securing the processes of product development, manufacturing, and delivery:
  - Is a written Risk Analysis available?
  - Are technical-organisational data protection measures selected according to the risk analysis

Service:

- Is a written Risk Analysis available?
- Are technical-organisational data protection measures selected according to the risk analysis?
- Does the documentation provide information on risks, vulnerabilities, etc?
- Does the product documentation provide information on the nature of the data that are being processed, allowing a sufficiently clear classification of data to allow adoption of the appropriate security measures?

3.1.5.3 Documentation of Technical and Organisational Data Protection Measures

The basis for a proper implementation of technical and organisational measures is a documentation of the measures that are implemented or will be implemented. Such an element can be used to compare target measures with actual measures. The choice of measures is to be based on the risk analysis (see Section 3.1.5.2). As this document might contain classified information, it will usually not be publicly available. Thus, the duties and obligations of users and administrators should be set out in a separate document: see Section 3.1.5.4.

Relevant for:

- Products:
  - For products (mandatory)
  - For procedures of product development, manufacturing and delivery (optional)
- Services: (mandatory)

Relevant Questions:

Product:

- Does the product documentation (directed to users and administrators) provide an overview of implemented security and data protection measures?
- Does the company-internal product documentation (e.g., high-level-designs, specifications, etc.) contain information of implemented security and data protection measures?

Service, product development, manufacturing and delivery processes:

- Is a detailed written documentation of technical and organisational measures available?
- Are version history, authors, and persons responsible for enacting etc. available?

3.1.5.4 Documentation of Individual Obligations

In order for users and administrators to know their obligations and duties, these have to be documented and have to be readily available (e.g. work instruction or process description).

Relevant for:

- Products:
  - For products typically not relevant.
  - For procedures used during product development, manufacturing and delivery (optional)
- Services: For procedures used during processing of personal data (mandatory)

Relevant Questions:

Service, product development, manufacturing and delivery processes:

- Are obligations and duties of individuals documented?
- Is the documentation easily available/accessible for the individuals at any time (e.g., online)?

3.1.5.5 Inventory of Hardware, Software, Data and Media

In order to assess all data processing operations and check their compliance with data protection regulations, an inventory of hardware, software, data and media used for the processing of personal data is necessary. As some of this information is also necessary for notification purposes (cf. Section 2.5.1), relevant documentation can be put down in a single document.

Relevant for:

- Products:
  - For products (mandatory)
  - For procedures of product development, manufacturing and delivery (optional)
- Services: (mandatory)

Relevant Questions:

Product:

- Does the product documentation provide information about the structure of data sets and -files containing personal data?

Service, product development, manufacturing and delivery processes:

- Is an up-to-date inventory of assets (or are several separate inventories) available, listing all the hardware, software, personal data and media?
- Does the documentation also provide information about connections of the assets via networks (network topology, domains, etc.) internally and to external networks?

3.1.5.6 Media Management

Media that store personal data are e.g., CDs, DVDs, tapes, diskettes, and USB memories.

Relevant for:

- Products:
  - For products (mandatory)
  - For procedures of product development, manufacturing and delivery (optional)
- Services: (mandatory)

Relevant Questions:

Product, Service, product development, manufacturing, and delivery processes:

- Do media that store personal data allow the identification of the type of information contained? Are they catalogued and stored in a place with access restricted to the personnel authorised by the security policy document?
- Does a media entry register exist that includes, directly or indirectly, information on the kind of medium, serial number of the medium, the type of information stored, and, if it has been sent in: the date and time of the sending of the medium, the sender, the means of delivery used, and the person responsible for receiving the medium (i.e., the person who signed for receipt)? Or if it has been created in-house, the date and time of its creation, the person creating the medium (i.e., who entered or copied the data onto it), and the person who logged the medium in the register?
- Does there exist a media exit register that includes, directly, or indirectly, information on the kind of medium that was sent out, the serial number of the medium, the type of information stored on it, the date and time it was sent out, the consignee, the means of delivery used, and the person responsible for receiving the medium?

3.1.5.7 Appointment and Duties of Data Protection or Security Officers

Relevant for:

- Products:
  - For products typically not relevant.
  - For procedures of product development, manufacturing and delivery (optional)
- Services: (mandatory)

Relevant Questions:

Service:

- Has an independent Data Protection Officer or Security Officer been appointed in line with national legislation? Does he or she carry out his or her job free of role conflicts and does he or she have the power needed to ensure compliance?
- Does he or she conduct audits on a regular basis, in which he or she checks compliance with the relevant security policies (Section 3.1.5.1), technical and organisational data security measures (Section 3.1.5.3) and individual obligations (Section 3.1.5.4)?

3.1.5.8 Instruction and Confidentiality of Personnel

When personal data are processed by human beings, the relevant persons have access to confidential data. These persons (usually staff members or staff members of agents such as Electronic Data Processing companies) have specific obligations of confidentiality that last longer than the actual employment.

Relevant for:

- Products:
  - For products typically not relevant.
  - For procedures of product development, manufacturing and delivery (optional)
- Services: (mandatory)

Relevant Questions:

Service, product development, manufacturing and delivery processes:

- Are new employees instructed/trained about their duties and obligations?
- Are employees regularly re-instructed/re-trained, e.g. once a year?
- How is the instruction/training carried out: Written material? E-Learning? Presentation? Practical exercises?
- Are the time and attendance of such instructions/trainings recorded (i.e., is a list kept of those that attend)?
- Are the duties and undertakings to abide by them formally recorded, in writing? Is a breach of these duties and undertakings a disciplinary matter? Is this made clear (e.g., in the contract of employment or a separate document linked to this contract)?

3.1.5.9 Data Protection and Security Audit

Technical and organisational data protection measures have to be monitored in detail on a regular basis in order to assess their effectiveness. Such audits can be carried out by either internal or external experts. Audits will often not only check effectiveness of measures, but also efficiency. Some national regulations require mandatory third-party audits whenever the supervisory authorities demand that they be carried out.

Relevant for:

- Products:
  - For products typically not relevant.
  - For procedures of product development, manufacturing and delivery (optional)
- Services: (mandatory)

Relevant Questions:

Service, product development, manufacturing and delivery processes:

- Are data protection/data security measures being monitored on a regular basis? How often, in which intervals and by whom?
- Is a written report available? Is a public version available (Online? Free of charge?)?

3.1.5.10 Incident Management by Manufacturers and Operators

An organisation must have management procedures to react adequately to security or data protection incidents or vulnerabilities. This includes proper documentation of incidents of the recovery proceedings and the information of customers. The objective of incident management is to provide information to enable a learning process to prevent further incidents as well as to support customers to avoid incidents. Additionally, procedures should be in place to manage security vulnerabilities before they become incidents.

Relevant for:

- Products:
    - For products operational (after sales) support by the manufacturer has to be offered in case of security or data protection related vulnerabilities (mandatory)
    - For procedures of product development, manufacturing and delivery (optional)
- Services: (mandatory)

Relevant Questions:

Product:

- Does the manufacturer offer support in cases of security or data protection related incidents or vulnerabilities? Does this include customer information (e.g., web, newsletter) on incidents/vulnerabilities, advice how to deal with them and providing patches/updates?

Service, product development, manufacturing and delivery processes:

- Are plans in writing available, setting out the relevant actions and procedures to be followed in case of an incident? Do they clarify the personnel responsible and their respective roles, etc.? Is support by manufacturers included in these plans?
- Is a record kept of incidents, the details of such incidents, and the recovery proceedings followed for each incident? Is this record available? To whom?
- How is information on security vulnerabilities collected (e.g., via manufacturers, CERT messages etc.) and how is this information dealt with (e.g., has a management team been set up)?

3.1.5.11 Test and Release

Before IT products are used, they have to be tested and formally released. For tests, dummy data or anonymous data must be used. Only in exceptional cases can real data be used. Tests have to be documented and should cover not only the intended use, but also trials of unauthorised use, incorrect input data, etc. Test and Release can be combined with prior checking (Section 2.5.2; see also Section 3.1.8 dealing with the documentation of the product and its installation).

Relevant for:

- Products:
  - For products (optional)
  - For procedures of product development, manufacturing and delivery (mandatory)
- Services: (mandatory)

Relevant Questions:

Product:

- Does the product provide test mechanisms (e.g. test accounts, dummy data, etc.)?
- Does the product provide for reliable erasure of test data (including logging files) after the testing?

Product development:

- Does the product development process contain quality assurance mechanisms such as formal tests as well as formal release procedures?

Service:

- Are procedures and software released in a formal procedure?
- Are tests planned and conducted before release?
- Are test data (e.g. anonymous data, dummy data etc.) used?
- Are tests and release decisions documented?
- Does the service provide mechanisms for reliable erasure of test data (including logging files) after the testing?

3.1.6 Disposal and Erasure of Data

Personal data have to be erased when they are not needed any longer. This is relevant for the regular deletion of personal data after general retention periods (see also Section □) as well as the individual deletion of personal data (e.g., deletion of inaccurate data according to Article 12, paras. (b) of Directive 95/46/EC, see also Section 4.1.4) and with regard to disposal of hardware, software or media storing personal data.

Relevant for:

- Products:
  - For products (mandatory)
  - For procedures of product development, manufacturing and delivery (optional)
- Services: (mandatory)

Relevant questions:

Product and Service:

- Can both complete data sets and individual pieces of data be erased?
- Can the erasure be documented (e.g., in a log file) in a manner *not* revealing the erased data?
- Does the product offer automated functionalities for erasure (e.g., timer or reminder functionality), for erasure after (fixed or relative or conditional) deadlines?
- Does the product erase data in such a manner that they cannot be recovered any more (e.g., by overwriting data on a hard disk, CD-RW, etc.)? Is the erasure method reliable and effective?
- Is it necessary to remove or sanitize parts of hardware before disposal or withdrawing from service (e.g., removal of hard disks from computers, flash memory from routers, etc.)?
- If physical destruction is used (e.g., for getting rid of paper, media, CD-ROM, chip cards, tokens): Is the method reliable and effective?
- If third party equipment is used for the processing of personal data (e.g., leased copying machines and their built-in hard disks): What measures have been taken to ensure that no personal data remain if the devices are returned (or repossessed)?
- Are media sanitized or destroyed before disposal? If third party services are used for this task: Is this legally permitted (see Section 2.4.1)? Are those third parties reliable? How is this ascertained (e.g., membership in a trade organisation with relevant codes of practice and monitoring/disciplinary procedures).
- Are the methods used for physical destruction (paper, media, CD-ROM) or logical destruction (overwriting) reliable and effective?

3.1.7 Temporary Files

If temporary files or -data are created, access to these data has to be controlled in the same manner as access to ordinary data. Temporary data have to be erased when they are not used any more.

Relevant for:

- Products:
  - For products (mandatory)
  - For procedures of product development, manufacturing and delivery (optional)
- Services: (mandatory)

Relevant Questions:

Product and Service:

- Does the product or the service create temporary files (e.g., temporary copies of documents processed by word processing software)?
- Is access to these data/these copies controlled by the product or within the service (e.g., by file permissions only for the user who actually processed the original document)?
- Are temporary files or -data erased automatically?
- Is this done in a secure manner (see section 3.1.6)?
- Does an automated procedure exist which warns that some temporary files were not properly closed/removed, and which then offers the possibility of their reliable erasure?

3.1.8 Documentation of Products and Services from a Customer's Perspective

Customers and users of certified IT products or IT-based services must comply with their national data protection laws and regulations if they are controller or processor. For this purpose, they need information to allow them to correctly fulfil their duties - e.g., notification (Article 18, 19 of Directive 95/46/EC), prior checking (Article 20 of Directive 95/46/EC), establishing appropriate security measures, etc.

Furthermore, controllers, processors as well as other users (e.g., consumers) might be obliged or should have an interest to operate an IT product or an IT-based service in a secure environment or to follow additional security procedures (e.g., to use of a virus scanner when using a webmail interface).

Relevant for:

- Products:
  - For products (mandatory)
  - For procedures of product development, manufacturing and delivery (optional)
- Services: (mandatory)

Relevant Questions:

Product:

- Does the documentation provide both sufficient and easily accessible information necessary to describe the types of processed data, functionalities, and interfaces with third parties, etc., of the product/service for internal/external documentation? E.g. a hypertext help file might be easy to use for practical work, but is difficult to use for the development of written documentation of security functions: compare Section 3.1.5.3).
- Does the documentation provide sufficient information on how to install the product properly (i.e., installation in such a way that the product´s data protection mechanisms are properly configured and used)?

- Is the documentation of the product easy to use both for administrative personnel and for other users? Does it contain information for secure use and configuration, e.g. on backups, passwords, changing default passwords, etc.? (NB: This question relates to content of data protection and security functions, not to general content.)

Service:

- Does the service provide all documentation needed by their clients to fulfil their duties (e.g., as concerns technical-organisational measures, their security concept, information about further [sub-]contractors, esp. in other countries, etc.)?
- Does the documentation provide sufficient information on how to use the service properly and how to configure service components securely and privacy friendly (e.g., on backups, passwords, changing default passwords, automated deletion, etc.)? Is the documentation easy to use both for administrative personnel and for other users?

3.2 Technology-specific and Service-specific Requirements

3.2.1 Encryption

Some national regulations explicitly require the encryption of personal data as a technical measure, e.g., for transmission via a network or when stored on mobile devices such as notebooks. Furthermore, encryption may be used to implement access control mechanisms, e.g. for data bases and backup storage.

Relevant for:

- Products:
  - For products (mandatory)
  - For procedures of product development, manufacturing and delivery (optional)
- Services: (mandatory)

Relevant Questions:

Product and service:

- Is encryption used appropriately for data transport via media and insecure networks?
- Is encryption used for access control (e.g., data bases or back-up)?
- If encryption is not included in the product, is advice for the user given in manual?
- Is the encryption effective? (key length, well known algorithms, etc.)
- How are encryption keys managed?

- What happens if keys get lost / forgotten?
- Are keys transmitted in a secure manner (e.g., keys for hard disk encryption of hosted servers)?

3.2.2 Pseudonymisation and Anonymisation

(Rec. 26, Article 6(1)(e) of Directive 95/46/EC)

Products and Services should process as few personal (i.e., identifiable) data as possible (see Section 1.2.1). Among several possibilities, anonymisation (depersonalisation) and pseudonymisation (aliasing) can be used to achieve this; these either completely sever the link between the data and any identifiable person, or they conceal this link by using intermediary identifiers.

The evaluation must address whether the methods used in this regard are effective and whether information leading to the disclosure of aliases is effectively protected.

Relevant for:

- Products:
  - For products (mandatory)
  - For procedures of product development, manufacturing and delivery (optional)
- Services: (mandatory)

See Section 1.2.1, above.

3.2.3 Technical Data Protection Functionalities Required by Directive 2002/58/EC

See Section 4.2, below

3.2.4 Ensuring Transparency of Automated Individual Decisions

Automated individual decisions based on personal aspects such as performance at work, credit-worthiness, reliability, conduct, etc. are limited by the Directive 95/46/EC in two ways:

a) Data subjects have the right to be informed about the logic of the data processing and decision making and

b) Individual cases must be taken into account, e.g., by giving the possibility of counterstatement and basing decisions not solely on automated methods.

(Rec. 41, Article12 (a) of Directive 95/46/EC)

Relevant for:

- Products:
  - For products (mandatory)

  - For procedures of product development, manufacturing and delivery (optional)
- Services: (mandatory)

Relevant Questions:

Product:

- Does the product (excluding far fetched scenarios of (ab)use) support the taking of fully-automated individual decisions that significantly affect the data subject(s)? If so:
  - Does the manufacturer inform the data controller about this issue and give advice for compliant operations?
  - Is the data subject informed of this? By the controller or user automatically, or only on request? (or not at all?)

Service

- Does the service support or involve the taking of fully-automated individual decisions that significantly affect the data subject(s)? If so:
  - Is information about this issue available for the data controller/operator, and advice give and documented for compliant operations?
  - Is the data subject informed of this? By the controller or user automatically, or only on request? (or not at all?)
  - Is the data subject informed of the matters that are taken into account in this? By the controller or user automatically, or only on request? (or not at all?)
- Can the data subject challenge this decision and, e.g., put forward counter-arguments or challenge the truth or significance of the matters taken into account? If so:
  - Is the decision then reviewed by a human person? With that human person actually taking a fresh look (rather than just “going through the motions”)?
  - What is the procedure (a) for using the service or product in this way, and (b) for dealing with any such challenge?
  - Is a prior check required by the relevant DPA? Has this been requested and done?

Set 4: Data Subjects' Rights

Set 4 lists the criteria to be applied in assessing the practical implementation of the **rights of the data subjects**. In particular, it deals with the right to be informed and the rights of access, correction, erasure and blocking guaranteed by Directive 95/46/EC. Furthermore, this set also concerns rights entitled by Directive 2002/58/EC (e.g., the right to confidentiality of communications and the right to be informed of security risks).

4.1 Rights under the Directive 95/46/EC

4.1.1 Right to Be Informed

(Articles 10 and 11 of Directive 95/46/EC)

Relevant Questions (for both 4.1.1.1 and 4.1.1.2):

- Are data subjects informed by the controller as required by Article 10 or 11 of Directive 95/46/EC respectively? If yes:
  - Does the information include
    - the identity of the controller and of his representative (if any),
    - the purpose(s) of the processing (i.e., not only the primary purpose(s) for which the data are collected but also any other, non-obvious, secondary purpose(s)),
    - the recipients or categories of recipients to whom the data are disclosed,
    - the categories of data concerned,
    - information whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
    - the existence of the right of access to and the right to rectify the data concerning him?
  - What other information is readily provided?
  - If no:
    - Does the data subject already have the information?
  - Are there special measures to enhance transparency? Can specific processing steps be clarified to the data subject?

4.1.1.1 Information Provided to Data Subjects when Data are Collected from them Directly

(Recital 38, Article 10 of Directive 95/46/EC)

Relevant Questions:

- What information is provided by the controller to the data subject at the time of data collection?
- How is this provided (e.g., in a questionnaire when the latter is used to collect data on the data subject, or through a "pop-up box" on a website)?
- Is the data subject's attention especially drawn to this information (or is it half-hidden, e.g., in small print in a legal document or page)?

4.1.1.2 Information Provided to Data Subjects when Data are Collected from other Sources

(Article 11 of Directive 95/46/EC)

Relevant Questions:

- What information is provided by the controller to the data subject, and when is this information provided?
- How is this provided (e.g., in a letter, or an email, or by means of a link to a website, included in an email)?
- How clear is it – in particular, will the data subject readily appreciate that the sender of the message has obtained information on him or her from a third party?
- If no information is provided: Are there any reasons that can justify this (e.g., Art. 11 (2) of Directive 95/46/EC)?

4.1.2 Right of Access

(Article 12(a) of Directive 95/46/EC)

Relevant Questions:

- Does the product or service support efficiently access by the data subjects to their personal data? Is this done by automated means to make this as quick and easy as possible? (but see the 4th bullet-point, below)
- Is access provided to all relevant information, i.e. in particular to:
  - all the data on the data subject
  - all purpose(s) of the processing
  - all sources and categories of recipients
  - details of processing by processors
  - details of the logical structure of the database

- Can all data on the data subject be easily retrieved in order to comply speedily and effectively with an access request?
- How is the identity of the data subject checked/authenticated?
- Are disclosures of data logged? Also as concerns disclosures to the data subject in the context of access requests?

4.1.3 Right of Correction

(Article 6(1) (d) and Article 12, paras. (b) and (c) of Directive 95/46/EC)

Relevant Questions:

- Are functionalities (in the case of IT products) or processes (in the case of IT services) in place allowing for the correction of data?
- Are errors automatically corrected?
- How are appropriate and immediate rectifications otherwise ensured?
- How is the quality of such corrections ensured?
- How is the identity of the data subject requesting a correction checked/authenticated?
- Are previous recipients of the data informed of the corrections? All of them? Always? Or does this depend on certain matters (like time or purpose)? If so, on what? Is the data subject involved in/consulted on this?

4.1.4 Right of Erasure

(Article 6(1) (d), 12, paras. (b) and (c) of Directive 95/46/EC)

Relevant Questions:

- If data are to be destroyed or erased, how is this done? Is the erasure complete and irreversible? How are unintentional copies avoided, such as copies created within an erasure function?
- Can data be selectively erased (e.g., parts of data records that are not needed anymore)?
- Are data erased by overwriting? Is this overwriting adequate?
- How is erasure affected in respect of back-up data?
- Are previous recipients of the data informed of erasures? All of them? Always? Or does this depend on certain matters (like time or purpose)? If so, on what? Is the data subject involved in/consulted on this?
- How are erasure-deadlines or re-presentation of data for consideration of erasure deadlines supported?

4.1.5 Right of Blocking

(Article 12, paras. (b) and (c) of Directive 95/46/EC)

Relevant Questions:

- Can data be marked (flagged) in such a way as to prevent their use for ordinary processing, while keeping them in the database? How is this done?
- How is such blocking logged (date and time, person responsible for ordering the blocking, etc.?

4.1.6 Right of Objection to Processing

(Article 12, paras. (b) and (c) and Article 14, paras. (a) and (b) of Directive 95/46/EC)

Relevant Questions:

- With respect to the intended marketing countries, does the national law of the EU Member States give the data subject a general right to object to processing?
- On what basis can a data subject object?
- Are there technical means to support the exercise of the right to object to processing? If so, what are they? In the case of IT-based services: Are appropriate processes established?
- Are objections passed on to previous recipients of the data? How is this done? What data are disclosed in the process of passing objections on? Is the data subject consulted on/involved in this?
- How does the national law of the EU Member States regulate the right of objection to processing of data for the purposes of direct marketing? Are mechanisms in place ensuring compliance with these requirements?

4.2 Rights under the Directive 2002/58/EC

4.2.1 The Right to be Informed of Personal Data Breaches

(Article 4(3) of Directive 2002/58/EC)

Relevant Questions:

- Does the person or company offering the service provide an electronic communications service, or is he or she a provider of a public communications network? If so:
  - What measures are taken to enable the person or company to inform subscribers or individuals in the case of a personal data breach without delay?
  - Do these measures ensure that in the case of a personal data breach adversely affected subscribers or individuals may be informed about the nature of the personal data breach and the contact points where more information can be obtained? Do they also ensure that measures to mitigate

the possible adverse effects of the personal data breach are recommended to subscribers or users?

4.2.2 The Right to Be Informed of Security Risks

(Article 4(2) of Directive 2002/58/EC)

Relevant Questions:

- Does the person or company offering the service provide an electronic communications service, or is he or she a provider of a public communications network? If so:
  - Does the person or company have adequate systems in place to safeguard the security of the product or service?
  - Can the person or company identify security risks adequately and sufficiently quickly?
  - What measures are taken to enable the person or company to inform users and subscribers of such risks?
  - Are the subscribers actually informed of such risks? Are there any recent examples?

4.2.3 The Right to Confidentiality of Communications

(Article 5, paras. (1) and (2) of Directive 2002/58/EC)

Relevant Questions:

- Does the product or service involve the use of electronic communication services or networks (such as telephone, fax or email)?
- Are adequate measures in place to prevent listening, tapping, storage or other kinds of interception or surveillance of those communications and/or of the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised? (cf. the fifth bullet-point, below)
- If the data are (temporarily) stored for technical reasons, is this without risk to the principle of confidentiality? How is compliance with this principle ensured in that regard?
- What measures are taken to ensure that recording (etc.) supposedly in accordance with the law (e.g. to prevent fraud) is actually compliant with the law? E.g. are there logs, prior authorisation requirements and/or ex post facto supervision?
- What measures are taken to create a secure (i.e., tamper-free) record of any handing over of recordings, or other communication details (including traffic data or geolocation data), to law enforcement agencies (including the police, the security services, and other, specialised agencies such as customs or the border police)? Does this record include details of, e.g., the date and time of the order to hand over the data, the authorising authority (e.g., a court), the order itself (number etc.)? Is there a procedure in place on how to handle such orders? Who can/must authorise, or at least sign off on, the handing over of the

data? Does he or she attest this in writing? In the record? Is the creation of such a record (a) required, (b) permitted, (c) prohibited, or (d) dependent on the terms of the order in question? Are such orders (the issuing of such orders) subject to independent scrutiny (e.g., by an independent Interception Commissioner, as in the UK)?

4.2.4 The Right to Receive Non-itemised Bills

(Article 7 of Directive 2002/58/EC)

Relevant Questions:

- Does the product or service involve billing for electronic communication services or value-added services? If so:
    - What alternatives are offered to subscribers to receiving fully-itemised bills?
    - How are subscribers informed of these options, and how can they choose such alternatives? Are these options free of charge?
- If not:
    - Are there effective measures in place to ensure that no details of the use of such services are recorded or retained, in a way that identifies the user?

4.2.5 The Right to Prevent Calling Line and/or Connected Line Identification and Call Forwarding

(Articles 8 and 11 of Directive 2002/58/EC)

Relevant Questions:

- Does the product or service involve the offering of electronic communications, including in particular landline and mobile telephone communications? If so:
    - Does the product or service offer "simple" and "easy" means to the user and subscriber to use the options mentioned above? Is this free of charge?
    - Are subscribers and users alerted to these options? How and when?
    - Is the general public made aware of these options? How and when?

4.2.6 Special Rights Regarding Directories of Subscribers to Electronic Communications Services

(Article 12 of Directive 2002/58/EC)

Relevant Questions:

- Does the product or service take the form of (or relate to) a public directory of subscribers to an electronic communications service? If so:
    - What is the purpose of the directory?

- What form does it take (book, CD-ROM, on-line)?
- Are there enhanced facilities in the directory, such as, e.g., reverse search possibilities? If so, have the data subjects been informed of these, and consented to them?
- Conversely, are measures taken to ensure that certain uses (such as reverse searches) cannot be supported? How? How effective is this (i.e. can this be easily circumvented)?
- Can subscribers opt out of direct marketing use of their directory data? If yes: Can they opt out free of charge? How is effect given to such a choice?