



Asia-Pacific  
Economic Cooperation

---

**2005/SOM1/ECSG/DPM/003**

Agenda Item: III

## **Multi-Layered Notices Explained**

Purpose: Information

Submitted by: USA



**First Data Privacy Subgroup Meeting  
Seoul, Korea  
23-24 February 2005**



# Multi-Layered Notices Explained

A White Paper by

The Center for Information Policy Leadership

HUNTON &  
WILLIAMS



Privacy notices are the windows to how organizations collect, use, share, and protect the information that pertains to individuals. As information processes have become more complex, privacy notices have become very long, mirroring the complexity. The effect has been to obscure the content that individuals need to know when making judgments about with whom they will do business. This has been an impediment to on-line commerce.

This paper describes a framework for assuring that notices are both easy to understand and follow as well as complete. These objectives are achieved by layering up to three documents as part of a notices package. This approach, supported by an ad hoc group of civic, business and government participants, has been adopted by the European Union's Article 29 Working Party. The initial layer, to be used when collecting information where space is tight, alerts the individual to the collection, major purpose, and where to go for additional information. The condensed notices assist the individual in understanding a company's practices and comparing them to other companies' practices, while the longer notice acts as a complete guide for compliance purposes. It is our belief that multi-layered notices will help educate consumers in APEC economies as to how information that pertains to them is managed.

### **APEC Privacy Framework Notice Principle**

The APEC privacy framework includes a notice principle that states:

“Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information...”

A successful privacy notice is a prerequisite for all privacy regimes. To align notices with the international standard, the principle states that a compliant privacy notice should include:

- a. The fact that personal information is being collected;
- b. The purpose for which personal information is collected;
- c. The types of persons or organizations to whom personal information may be disclosed;

- d. The identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information; and
- e. The choices and means that the personal information controller offers individuals for limiting the use and disclosure of, as well as accessing and correcting, their personal information.

### **Current Notices Often Too Complex**

However, privacy authorities worldwide have found current privacy notices to be less than successful. Privacy notices were a focus of the 25th International Data Protection Conference held in Sydney, Australia, and were noted in the European Commission's review of the implementation of the EU privacy directive. The Acting US Comptroller of the Currency (regulator of national banks) made notices the subject of her speech given January 12, 2005. These authorities believe that the current privacy notices are often too long and complex, and that individuals often do not have knowledge about information practices after reading these long notices. Independent research by Yankelovich, “Privacy & American Business,” and others supports these findings.

Information processes tend to be very complex, and descriptions of how information is collected, used, shared and protected often match the complexity of the subject matter. An analogy might be helpful. Think about the system of waterways that not only drain a geography, but also support agriculture, transportation, fisheries, power generation, and recreation. Try describing the path a raindrop follows in making its way from the drainage ditch to a stream, creek, river and finally the sea. It would be hard to write a description in a very short, easy-to-read document, especially if one wanted to describe all the potential uses and users that might touch that drop.

Similarly, information that pertains to us is personal and its potential uses complex, yet we want some sense of what is going on. With this in mind, the Center for Information Policy Leadership (“CIPL”) and its member companies in 2001 began work on making privacy notices more effective for individuals and, therefore, to enhance public trust and participation.

## Lessons from Food Label Research

The group first looked at the research conducted in the 1980s to inform the creation of nutritional food labels. That research tells us:

- Notices must be short. Consumers get lost if presented with too much information. Notices should therefore discuss no more than seven discrete topics;
- Notices must use language that is so common that individuals are not required to translate what they read into what they understand. The words must be those that they use with their neighbors;
- Notices must rely on long and short-term memories working together. The notice seen yesterday must help consumers understand the notices they see today. A common format that makes use of a common graphic interface accomplishes this objective.

The research suggests a privacy notice that is easily recognizable as a privacy notice; in a common format so individuals may easily find the information important to them; in everyday language; and short with limited elements.

## Using Layering to Accomplish Both Readability and Completeness

However, to define fully a complex organization's information practices, a notice must also be complete. How does one reconcile completeness with something that is short and easy to read and understand? Increasingly, organizations find that the answer lies in multi-layers. A multi-layered notice has two or more layers that work together to give the individual complete information in a manner in which one can understand information use and make choices. Layered notices were first suggested by CIPL in December 2001 at a workshop sponsored by US financial services regulatory agencies. This approach became the subject of a resolution adopted by international data protection commissioners in September 2003 (appendix A), and further refined by a March 2004 workshop that included government, civic society and business interests. The conclusions from that workshop were captured in the "Berlin Memorandum" (appendix B). The

data protection commissioners from the 25 European Union member states adopted this approach on December 7, 2004 (appendix C).

The European data protection authorities suggest a notices system comprised of three layers:

- The short notice — The party collecting information, principle purpose, and where to go for more information and choices (example 1);
- The condensed notice — A snapshot of an organization's information practices in a common, graphic format (examples 2 & 3); and
- The full notice — All information required by data protection laws or codes of conduct.

### Please see example 1 — a short notice on a PDA screen.

The short notice would be used when collecting information where space is an issue, like a mobile phone. The condensed notice would be used on websites or in hard copy for off-line transactions. The complete notice would be provided on request and could be hyperlinked on-line.

The Center for Information Policy Leadership developed a basic template for the condensed notice that was used in the examples that were included with the EU common position, and that are/is currently in use at a number of websites. The model includes six boxes with headings:

- Scope — The parties covered by the notice;
- Personal Information — Information collected directly from the individual and from third parties;
- Uses and Sharing — A summary of uses by the organization collecting the information and others;
- Choices — The choices that individuals have to limit sharing and gain access to the information held by the organization, and how to exercise those choices;
- Contacts — How to reach the organization for the more complete notice;

→ Other Important Information — Information important to the individual, including seal programs and other systems for accountability.

These categories are flexible enough to cover all the notice categories suggested by the APEC Privacy framework.

**Please see examples 2 and 3 — examples of template notices currently or soon to be on websites.**

The advantage of multi-layered notices is that a single document is not being asked to achieve multiple objectives. The short notice notifies the consumer that information is being collected. The condensed notice gives the individual a snapshot of an organization's information practices, his options, and means of exercising those options. The complete notice defines purpose limitations and provides complete information on the organization's information practices. The total package communicates clearly while being complete. Compliance would be determined not by a single element, but rather by the total package.

**Focus Group Testing**

The template-based notices have been tested with focus groups in the US, Germany and Hong Kong. The US research was led by P&G and conducted in Cincinnati, Ohio. That research, conducted over two years (2002-2003), found that 1) consumers believed that long notices were obscuring important information and 2) that they preferred the template that allows them to compare the practices of different companies.

The research in Germany and Hong Kong was conducted by MSN in 2004. That research determined that Hong Kong residents are too busy to read long notices, and therefore prefer the shorter, more graphically interesting template-based notice.

Germans feel compelled to read long notices, but find them too long and complex. They too prefer the template-based notice.

**Please see example 4 — MSN Hong Kong test notice.**

**The Center for Information Policy Leadership Recommendations**

The Center for Information policy Leadership suggests that the ECSG adopt multi-layered notices as a best practice for complying with the notice principle contained in the APEC framework. Furthermore, we would recommend that multi-layered notices be used in the implementation workshops to demonstrate how the notice principle may add value and confidence to electronic commerce. Consumers are more willing to participate in markets if they trust participants and readable notices enhance consumer trust.

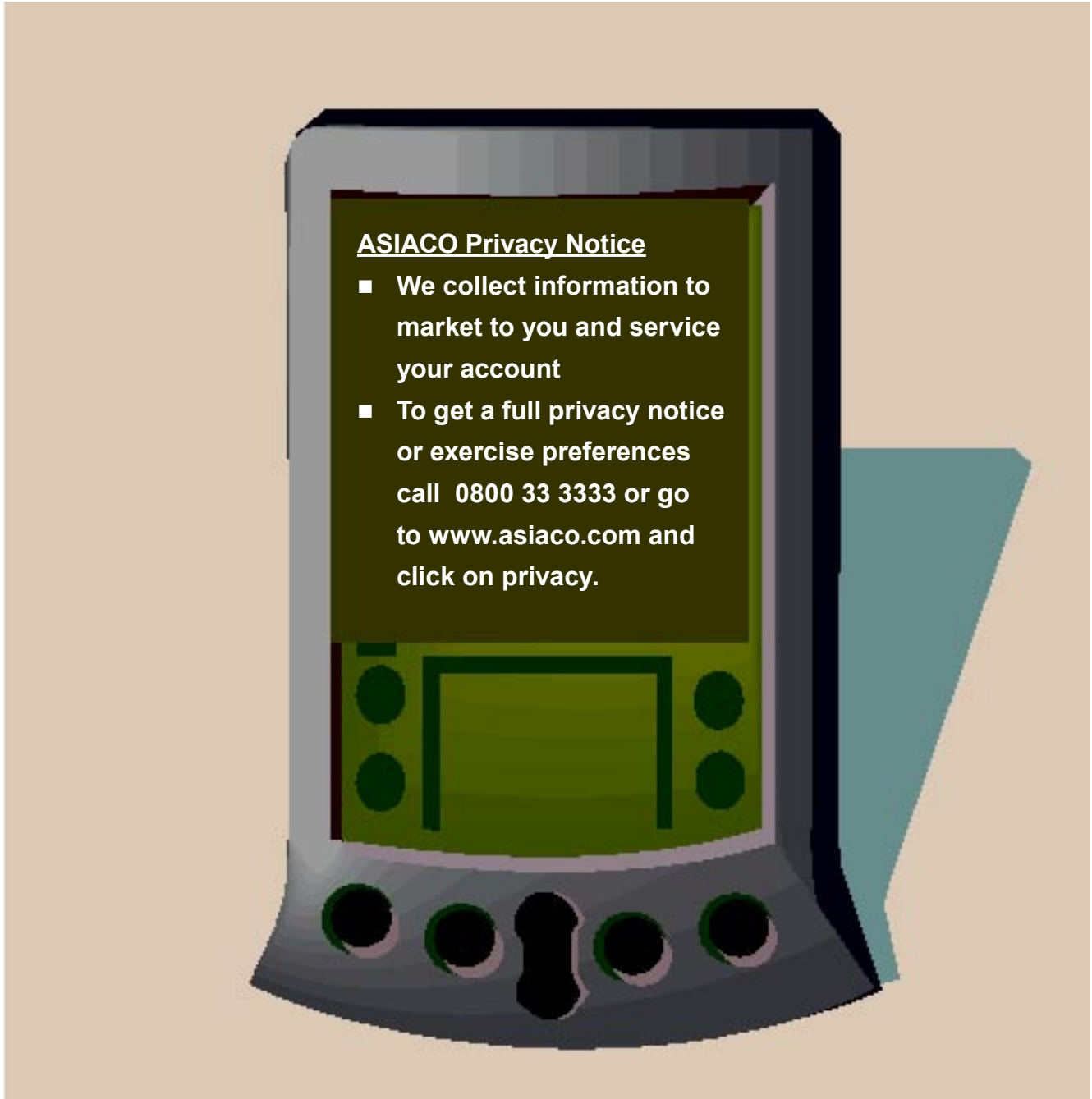
**Examples**

1. PDA short notice
2. Proctor & Gamble website notice
3. IBM website notice
4. MSN Hong Kong test notice

**Appendix**

- A. Sydney Resolution
- B. Berlin Memorandum
- C. Article 29 Working Party Common Position on Multi-Layered Notices

## Example 1



## Example 2-A P&G Korean Notice

<p style="font-size: 1.2em; font-weight: bold; margin: 0;">P&amp;G 개인 정보 보호 정책</p>	<p><b>적용 범위</b></p> <p>본 정책은 P&amp;G에서 운영하는 Procter &amp; Gamble Company(P&amp;G) 소비자 웹 사이트를 포함하여 본 정책이 게시된 웹 사이트에 적용됩니다.</p>
--	---

개인 정보	<p>• 저희는 귀하의 이메일이나 우편 주소와 같이 귀하가 자세한 내용을 보기 정보만을 수집합니다.</p> <p>• 저희는 브라우저 종류, 운영 체제, 저희 웹 사이트 관리를 지원하기 위하여 방문하는 웹 페이지 등과 같이 개인 정보와 무관한 정보를 수집합니다.</p> <p>• 저희는 웹 사이트와 이메일 프로그램을 관리하기 위하여 쿠키 및 다른 인터넷 기술을 사용합니다. 개인 정보를 수집하거나 저장할 목적으로 이 기술을 사용하지 않습니다.</p> <p>• 다른 경로를 통해 저희가 귀하의 인구 통계 및 생활 양식 정보와 같은 추가 정보를 얻을 수 있습니다.</p>
-------	--

사용	<p><b>보기</b></p> <p>• 저희는 다음과 같은 목적을 위하여 여러분이 제공하는 정보를</p> <ul style="list-style-type: none"> <li>• 귀하가 요청하는 정보 및 샘플 제공</li> <li>• 유익한 웹 사이트 경험 제공</li> <li>• 귀하의 요구에 맞는 신제품 및 서비스 개발</li> </ul> <p>• 저희가 명시적으로 요청하여 동의를 얻은 경우가 아니면 귀하의 개인 정보를 다른 마케팅 담당자와 공유하지 않습니다.</p> <p>• 저희는 귀하의 정보 제공 이유에 해당하는 목적을 위해서만 귀하가 제공하는 개인 정보를 사용합니다.</p>
----	---

귀하의 선택	<p><b>보기</b></p> <p>• 저희 프로그램에서 귀하의 정보를 제거하려면 <a href="#">여기를 클릭</a> 하십시오.</p> <p>• P&amp;G에 제출한 개인 정보에 대한 공개 옵션을 지정하려면 <a href="#">여기를 클릭</a> 하십시오.</p>
--------	--

연락 방법	<ul style="list-style-type: none"> <li>• 온라인 개인 정보 보호 정책을 보려면 <a href="#">여기를 클릭</a> 하십시오.</li> <li>• 글로벌 개인 정보 보호 정책을 보려면 <a href="#">여기를 클릭</a> 하십시오.</li> <li>• 문의하실 내용이 있으면 <a href="#">여기를 클릭</a> 하십시오.</li> <li>• 우편을 이용하실 경우에는 아래 주소로 보내십시오. P&amp;G Privacy Team Two Procter &amp; Gamble Plaza TN-7 Cincinnati, OH 45202</li> </ul>
-------	--

중요한 정보	<ul style="list-style-type: none"> <li>• P&amp;G는 소비자와 협력하여 개인 정보 보호와 관련된 불만 사항이나 문제를 공정하게 해결하기 위하여 노력하고 있습니다.</li> <li>• 저희는 개인 정보 보호 문제가 발생했다고 판단되면 국가 데이터 보호 기관과 협력합니다.</li> <li>• 저희 미국 웹 사이트는 미국 <a href="#">Better Business Bureau OnLine® Privacy Seal</a>을 통해 개인 정보 보호 인증을 받았습니다.</li> </ul>
--------	--

링크

• 개인 정보 링크를 클릭하면 온라인 정책의 [저희가 수집하는 정보](#) 및 [정보 사용 방법](#) 페이지로 이동합니다.

• 사용 링크를 클릭하면 온라인 정책의 [저희가 수집하는 정보](#) 및 [정보 사용 방법](#) 페이지로 이동합니다.

• 귀하의 선택 링크를 클릭하면 [귀하의 선택 및 귀하의 정보 공개](#) 페이지로 이동합니다.

• 연락 방법 - 저희 온라인 개인 정보 보호 정책을 모두 보려면 [여기를 클릭](#) 하십시오. 온라인 정책 링크를 클릭한 후에 간략한 정책 설명 링크를 클릭해야 합니다.

• 저희 글로벌 개인 정보 보호 정책을 보려면 <http://www.pg.com/company/our-commitment/privacy-policy/privacy-policy.jhtml> 페이지로 이동하십시오.

• 문의하실 내용이 있으시면 온라인 정책에서 [전세계 연락처](#) 페이지로 이동하십시오.

## Example 2-B



### Procter and Gamble Company Privacy Notice Highlights

#### Scope

This statement applies to the **Procter & Gamble Company** and the [www.pg.com](http://www.pg.com) website.

#### Personal Information

- We collect information you choose to submit during your registration.
- We use common internet technologies such as cookies on our websites and emails.
- We sometimes obtain additional information about you, such as your demographic and lifestyle information, from other sources.
- For more information about our information collection practices please [click here](#).

#### Uses

- We use the information you submit to provide you with the service you requested.
- We use information about you to provide you with helpful and targeted offers from P&G products and services. [Click here](#) for more information.
- We do not share, trade, or sell information about you with other marketers without your permission. We may share your information with vendors we've hired to send you the offers you signed up for. [Click here](#) for more information.

#### Your Choices

- You may request to be removed from our programs by [clicking this link](#).
- You may request access to personal information you have submitted to P&G by [clicking this link](#).

#### Important Information

- The PG.com website has been awarded the [Better Business Bureau OnLine®](#) Privacy Seal. Please [click here](#) for more information.
- We take steps to protect the information you provide against unauthorized access and use. For more information [click here](#).

#### How to Contact Us

For more information about our privacy policy, go to the privacy statement on our website at:

[http://www.pg.com/privacy\\_full.html](http://www.pg.com/privacy_full.html)

Or write us at:

P&G Privacy Team  
One Procter & Gamble Plaza  
TN-7  
Cincinnati, OH 45202



# Privacy

IBM privacy practices on the web

## Scope

This statement applies to **IBM** Web Sites Worldwide.

## Personal Information

In general, you can visit us on the internet without telling us who you are or giving us personal information. There are times when we may need information from you, or instance: to process an order, to correspond, to provide a subscription or in connection with a job application. We may supplement this information to complete a transaction or to provide better service.

## Uses

- To fulfill your requests by us or by others involved in fulfillment.
- To contact you for customer satisfaction surveys, market research or in connection with certain transactions. By IBM and selected organizations for marketing purposes if you have permitted such use.
- In a non-identifiable format for analysis (e.g., Clickstream Data).
- To develop our business relationship if you represent an IBM Business Partner or Vendor.

## Your Choices

- When we collect information from you, you may tell us that you do not want it used for further marketing contact and we will respect your wishes.
- You may also turn off cookies in your browser.

## Important Information

IBM is a member of Truste ([www.truste.org](http://www.truste.org)). IBM abides by the EU/US Safe Harbor Framework. To correct inaccuracies in IBM's record of your personal information respond to the sender or contact IBM at [access\\_request@us.ibm.com](mailto:access_request@us.ibm.com).

For IBM's complete notice see [IBM's Privacy policy](#).

## How to Contact Us

Questions about this statement or about IBM's handling of your information may be sent to:

[prvcy@us.ibm.com](mailto:prvcy@us.ibm.com), or

Privacy, IBM, 1133 Westchester Avenue, White Plains, NY 10604.

### Example 3

## Example 4

MSN Home | My MSN | Hotmail | Shopping | Money | People & Chat

最近更新：2004年10月

# msn Summary 私隱權注意事項



附圖：此份注意事項是完整 MSN 私隱權聲明 的部分面圖。此份主要事項和完整私隱權聲明適用於 MSN 網站和服務。

**個人資訊：**

- 當您註冊某些 MSN 服務時，我們將要求您提供個人資訊。
- 我們收集的資訊可能與來自其他 Microsoft 服務或來自其他公司的資訊進行結合。
- 我們會追蹤您與我們網站和服務的互動情況，以提供個人化的使用體驗。

**資訊的使用：**

- 我們會使用收集的資訊來提供您所要求的服务。我们的服务可能包括针对个人举荐的订费和广告资讯。
- 我们会使用您的个人资讯来通知您 Microsoft 及其附属公司所提供的其他产品或服务，以及向与您相关的意见进行调查。
- 我们不会出售或租借顾客名单给任何的其他第三方。为了协助提供服务，我们偶尔也会提供资讯给代我们提供服务的其他公司。

**其他相关链接：**

**連絡資訊：**

若需我們私隱權政策的更多資訊，請參閱我們網站上的完整私隱權聲明 <http://privacy.msn.com/zh/>。或透過郵件與我們聯絡：

MSN Privacy  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052  
[privacy@msn.com](mailto:privacy@msn.com)

**您可以：**

- 工務至 MSN 主網頁的「設定網頁」選擇我們便可與您聯繫。
- 逕至 [knowshott@microsoft.com](mailto:knowshott@microsoft.com) (英文信箱) 或打「電子郵」。
- 逕至 [www.msn.com/zh/privacy](http://www.msn.com/zh/privacy) 檢視和編輯您的個人資訊。

**重要資訊：**

- 若需特定 MSN 服務的資訊，請參閱完整私隱權聲明中相關的附註和圖示。
- 我們使用 Microsoft .NET Passport 提供在 MSN 的註冊和登入服務。若需進一步了解 Passport 服務，請參閱 [Microsoft .NET Passport 私隱權聲明](http://microsoft.net/passport/zh/)。
- 若要檢視我們對兒童私隱權所採取的其他措施，請逕至完整私隱權聲明中的兒童版。
- 若需如何在網上保護您的個人電腦、收件匣、個人資訊和家人的相關資訊，請逕至我們的網上安全資源中心。

Try MSN Internet Software for FREE

MSN Home | My MSN | Hotmail | Shopping | Money | People & Chat | Search

© 2004 Microsoft Corporation. All rights reserved. Terms of Use. Advertisers: TRUSTe Approved Privacy Statement. GetHotWire

Feedback | Help

# Appendix A

## 25th International Conference of Data Protection & Privacy Commissioners

Sydney, 12 September 2003

Proposed Resolution on improving the communication of data protection and privacy information practices

**Proposer: Privacy Commissioner, Australia**

**Co-sponsors:**

- Commissioner for Data Protection and Access to Information, Brandenburg, Germany;
- Commission Nationale de l'Informatique et des Libertes, France
- Data Protection Commissioner, Czech Republic;
- Hellenic Data Protection Authority,
- Independent Centre for Privacy Protection, Schleswig-Holstein,
- State Data Protection Inspectorate, Republic of Lithuania,
- Dutch Data Protection Authority

**Resolution**

That the 25th International Conference of Privacy and Data protection Commissioners resolve that:

1. The conference calls the attention of organisations, in both public and private sectors, to the importance of:
  - improving significantly their communication of information on how they handle and process personal information;
  - achieving global consistency in the way they communicate this information;
  - and by these means
  - improving individuals' understanding and awareness of their rights and choices and their ability to act on them; and

- putting an incentive on organisations to improve, and make more fair, their information handling and processing practices as a consequence of this awareness.
2. The conference endorses the following means of achieving these goals:
    - development and use of a condensed format for presenting an overview of privacy information that is standardised world wide across all organisations which sets out:
      - the information that is most important for individuals to know; and
      - the information that individuals are most likely to want to know; and
    - the use of simple, unambiguous and direct language;
    - the use of the language of the website or form which is used to collect information;
    - confining the format to a limited number of elements which, consistent with the above, covers important data protection principles like:
      - who is collecting the personal information and how to contact it (at least the official name of the organisation and physical address);
      - what personal information the organisation collects and by what means;
      - the purposes for which the organisation is collecting the personal information;
      - whether the personal information is to be disclosed to other organisations and, if so, the kinds or names of organisations and for what purposes;
      - the privacy choices the individuals have and how to exercise them easily, in particular, choices about whether personal information can be disclosed to third

- parties for unrelated but lawful purposes and about which personal information individuals must provide to receive a service;
- a summary of the individual's rights of access, correction, blocking or deletion;
- which independent oversight body individuals may approach in order to verify the information given;
- the use of appropriate means to enable individuals to find further information easily including:
  - information that any applicable law requires an organisation to provide, including rights of access, correction, blocking or deletion, and how long an organisation retains personal information; and
  - a complete explanation of the information summarised in the condensed format; and
  - the complete statement of an organisation's information handling and processing practices.

3. The conference agrees that such standardised and condensed format should be consistent with all national laws that may apply, and is to be in addition to, where necessary, and consistent with, any notices that an organisation is legally required to give an individual.

4. The conference is aware of the importance of the timing of presentation of data protection and privacy information to the individual. For example, it is particularly desirable for information to be presented automatically at the point where individuals have the chance to choose what information they give, and whether information can be disclosed to third parties. In other cases it may be appropriate to leave individuals to seek data protection and privacy information via obvious links. The conference is aware of the important work the EU Article 29 Data Protection Working Party has done on the automatic presentation of data protection and privacy information in *Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union*.

5. The conference considers the timing for the presentation of the condensed format (which takes into account both the on and

off-line environments) would be a fruitful area of further work for Data Protection and Privacy Commissioners.

6. The Conference is also aware of related activities such as the development of computer languages describing privacy policies. It encourages the further development of ways to translate those policies into the standardised and condensed format.

7. The conference sees these as first steps to encourage better practice in the way organisations communicate privacy information about how they handle or process personal information. The conference is aware of initiatives in this area and encourages any such initiatives to improve communication between organisations and individuals. The Conference looks forward to working with organisations and interest groups that are taking such steps and it expects to take further steps to improve on communications between organisations and individuals in future conferences.

#### **Explanatory notes for Proposed Resolution on improving the communication of data protection and privacy information practices**

This resolution aims to reach agreement about the need for public and private sector organisations to better communicate information about the way they handle and process personal information.

#### **Why this resolution is important**

A significant number of countries around the world have privacy law, or other laws, that require companies and other organisations collecting personal information to give consumers information about their privacy practices. Ensuring people are well informed about what an organisation does with their personal information is one of the main ways that laws seek to protect privacy. This enables people to exercise choice and have control over their personal information.

This resolution is important because there is growing evidence, however, that despite the volumes of documents and information that organisations are providing, individuals are not well informed about the privacy practices of the organisations they deal with, (see for example, a recent report from the Annenberg Public

Policy Center of the University of Pennsylvania, *Americans and Online Privacy: The system is Broken* (<http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/new.html>) and that further work is needed to ensure that individuals get the information they need at the right time to place their trust in the sites with which they are interacting. (See for example, the *Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union* ([http://europa.eu.int/comm/internal\\_market/privacy/workinggroup/wp2001/wpdocs01\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/workinggroup/wp2001/wpdocs01_en.htm))). The Annenberg Public Policy Center research also provides evidence confirming that individuals will spend very little time and effort to find out about such information.

A further challenge is to enable individuals to be well informed and able to exercise choices when the organisations with which they are dealing operate globally. For example, Action 6, “More harmonised information provisions” in the recent European Commission *Report on the transposition of Directive 95/46/EC* calls for a more harmonised approach to providing notice to individuals ([http://europa.eu.int/comm/internal\\_market/privacy/lawreport/data-directive\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/lawreport/data-directive_en.htm)).

### What the resolution is trying to achieve

There is now considerable research on how organisations can improve communication with individuals when individuals need to be given important information. Much of this has happened in the area of food labelling. (See for example, James R. Bettman, John Payne and Richard Staelin, ‘Cognitive Considerations in Effective Labels for Presenting Risk Information’, *Journal of Public Policy & Marketing*, Vol 5, 1986, p.1-28.). However, there has also been quite a bit of work done in relation to better communicating information about an organisation’s personal information handling practices. Simplification of notification procedures is on the 2003 work program for the European Union Article 29 Data Protection Working Party. ([http://europa.eu.int/comm/internal\\_market/privacy/workinggroup/wp2003/wpdocs03\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/workinggroup/wp2003/wpdocs03_en.htm)). Work has also been done on improving notice in the US (<http://www.ftc.gov/bcp/workshops/glb/index.html>) and by the P3P user agent taskforce (<http://www.w3.org/P3P/2003/p3p-translation.htm>).

The result of this work shows that an important first step to improving communication in both the on and offline environment is;

- a shorter format for providing information, with a limited number of elements (some research says 6 or 7);
- including just the basic information that individuals want to and need to know;
- standardisation to develop familiarity, education and ability to compare;
- simpler, non-legalistic language, and use of everyday terminology;
- clear and easy access to further information.

This resolution focuses on these matters as being an important first step in improving communication. There are, however, a number of other very important dimensions to achieving this, which it not possible for this resolution to cover in detail.

The next important step is presenting information about an organisation’s information handling practices at the right time. Again, the EU Article 29 Data Protection Working Party has done a considerable amount of work on this particularly in the online environment in *Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union* ([http://europa.eu.int/comm/internal\\_market/privacy/workinggroup/wp2001/wpdocs01\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/workinggroup/wp2001/wpdocs01_en.htm)). Ensuring that the right information is presented at the right time is a complex area. The right time may vary depending on the medium the person is using to interact with an organisation. For this reason, the resolution proposes that this could be a fruitful area of future work for data protection and privacy commissioners.

Although the individual would be the main beneficiary of improved communication of information about an organisation’s privacy practices, there are also likely to be benefits for business. For example, organisations could achieve better relationships with their clients in the form of trust and loyalty. A standardised format that could be used by a company globally could provide economies of scale.

## The drafting process

Having identified the problem of inadequate communication of information about an organisation's personal information handling practices as being a possibly global issue, the Office of the Federal Privacy Commissioner, Australia, asked accredited data protection and privacy commissioners by email if they agreed that this was an important issue and an appropriate topic for a resolution at the 25th International Conference of Data Protection and Privacy Commissioners (<http://www.privacyconference2003.org/>). The Office then sent another email outlining the issue further. Eighteen out of the twenty-seven Commissioners who responded to these emails agreed that this was an important issue. On the basis of these responses the Office invited Commissioners from Brandenburg, Czech Republic, France, Greece, Hong Kong, Italy, Lithuania, Netherlands, Poland and the United Kingdom to form a working group to work on the draft of the resolution which is now circulated with this explanatory note.

Before the conference, the Office of the Privacy Commissioner, Australia created a webpage with background material on it. This material aims to help understanding of the debate about improving communication of information about privacy practices. This is available at <http://www.privacyconference2003.org/resolution.asp>.

The issues behind the resolution will also be discussed in a workshop session open to all registered participants in the 25th International Conference of Data Protection Commissioners, before Commissioners formally consider the resolution.

## Points about content of the resolution

The resolution assumes that organisations will comply with their notification requirements under the law. The standardised condensed format proposed in the resolution would (unless an organisation does not need to provide any more information) be in addition to these requirements.


Some people may be concerned that organisations should also be improving their information handling practices, or that the privacy laws applying to organisations should be strengthened.

These are very big issues that cannot easily be dealt with in one resolution. Instead, this resolution is taking one first and small, but achievable, step of seeking to achieve *effective communication* of information about the current handling practices of organisations. It deals with this communication issue as separate from the much more complex one of whether, for whatever reason, those practices need improving. Of course, the practices an organisation communicates about must be consistent with any applicable law.

The purpose of providing a condensed format is to greatly improve the chances that individuals will at least read and understand the most important privacy information. This would be an important practical improvement on the current situation which appears to be that many individuals do not read or understand very much of the information that organisations provide. The resolution therefore picks out the elements of information about an organisation's information handling practices identified by the working group as being the most important to be included, based on research to date and its own knowledge. There are, of course other important elements. However including them in the condensed format would make it too long and would defeat the purpose of the resolution which is to achieve effective communication. The resolution deals with this dilemma by urging organisations to provide appropriate means to enable individuals to find further information easily, including the all the rest of the information that the law may require an organisation to provide.

If a condensed format is to be standardised globally and across organisations, there are limits on the kind of information that can be included in the format. For example, laws about rights of access vary from country to country. Trying to set out all the possible applicable rights an individual might have globally in a condensed format would make it too long. The resolution approaches this problem by providing that the format should summarise access rights and then provide the means for individuals to find further information.

It is very important that the information an organisation includes in a condensed format does not mislead individuals about the organisation's practices. For this reason, the resolution provides that the condensed format must be consistent with all national



laws that apply, and this would include any laws prohibiting organisations from engaging in misleading and deceptive conduct. If organisations take sufficient care, information in the condensed format can be framed so that individuals can get an accurate snapshot of an organisation's practices. The resolution also addresses this issue by requiring the format to include information about the independent supervisory body to which individuals may complain if they are concerned that their rights have been breached.

Finally, the working group seeks to ensure that the work begun by passing this resolution does not end there. The final paragraph of the resolution therefore suggests that the way forward is for Commissioners to work with all those working on improving communication in the way suggested by the resolution to ensure that the next necessary steps are taken.

## Appendix B

### *Berlin Privacy Notices Memorandum*

Complex privacy (fair processing) notices aimed at consumers and citizens do not serve a useful communications purpose, since:

- Consumers and citizens find them too long and hard to understand, and therefore the notices do not facilitate effective consumer and citizen feedback;
- Companies and public bodies find them an impediment to building trust with their customers and citizens; and
- Regulators find that complex notices frustrate their policy objectives of raising awareness and improving compliance.

This is a problem that crosses sectoral and geographical boundaries. An international collection of twenty-three privacy and consumer experts from consumer organizations, data protection agencies, government privacy offices and a variety of industries met in Berlin on March 23, 2004 to address the issues. Recognizing that new architecture is needed for privacy notices, this memorandum is the result.

Effective privacy notices should be delivered within a framework with the following core concepts:

- **Multi-layered.** Privacy information cannot and should not normally be conveyed in a single document or message. Instead, information about an organization's privacy practices should be provided in a layered format. The "short" (condensed or highlights) layer should provide, in a highly readable format, the most important information that individuals need to understand their position and make decisions. Even shorter notice layers may be acceptable for coupons, mobile phone screens, and other places where notice is needed, but space is extremely limited. Additional information should then be easily accessible in longer, more complete layers. This approach improves both comprehension and legal compliance, because the privacy notice – the whole framework - can deliver content in a more

understandable fashion, and in a manner appropriate to the medium and the targeted audience.

- **Comprehension and Plain Language.** All layers should use language that is easy to understand. Comprehension by the target individuals is an important objective for privacy notices so they can understand what is being said, make informed decisions and have the knowledge and understanding to drive privacy practices.
- **Compliance.** The total notices framework (all the layers taken together) should be compliant with relevant law, while each individual layer must communicate the information necessary for the individual to make an informed decision at that point in time. It is especially important to draw attention to "surprises" - processing that goes beyond established or expected norms.
- **Format and Consistency.** Consistent format and layout will facilitate comprehension and comparison. Consumers learn through repetition and it is important that notices from both the private and public sector have a consistent format and layout to facilitate this learning. More discussion is needed on how to maintain consistency while still allowing for the differences that exist in various sectors.
- **Brevity.** The length of a privacy notice makes a difference. Research shows that individuals are only able to absorb a limited amount of material from a notice. The short layer should contain no more information than individuals can reasonably process. The consensus from the research is that no more than seven categories should be used with limited information in each category. The long layers may need to be long, if that helps with readability and completeness.
- **Public Sector.** These concepts have equal applicability to governmental collection and management of personal information.



## The short privacy notice

---

The short notice should be the initial notice that an individual receives (online or in paper form) when personal information is first sought. The goal of this notice should be to provide the essential information in a highly readable and (within the sector) comparable format. The short notice should include:

- Who the privacy notice covers (i.e., who is the responsible person or entity);
- The types of information collected directly from the individual and from others about the individual;
- Uses or purposes for the processing;
- The types of entities that may receive the information (if it is shared);
- Information on choices available to the individual to limit use and/or exercise any access and/or other rights, and how to exercise those rights; and

- How to contact the collector for more information and to complain (to the collector and to an independent oversight body if appropriate).

The short privacy notice should be formatted in a consistent fashion that makes it easy for the individual to find the above elements that are important to them. While notices will be different from organization to organization and from sector to sector, similarity in format will facilitate individual knowledge and choices. U.S. focus group research has shown that consumers prefer boxes with bold headings.

The complete notice would include all the details required by relevant laws. It should still be as readable as possible and written in language that is easy for the individual to understand.

This memorandum was prepared by the session conveners: Martin Abrams, Malcolm Crompton, Alexander Dix, and Richard Thomas.

# Appendix C

ARTICLE 29 Data Protection Working Party



11987/04/EN  
WP 100

## Opinion on More Harmonised Information Provisions

**Version: November 25 2004**

For

- Discussion
- Adoption

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate E (Services, Copyright, Industrial Property and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.

Website: [www.europa.eu.int/comm/privacy](http://www.europa.eu.int/comm/privacy)

## OPINION

### **MOVING FORWARD ON ACTION 6 OF THE WORK PROGRAMME FOR A BETTER IMPLEMENTATION OF THE DATA PROTECTION DIRECTIVE MORE HARMONISED INFORMATION PROVISIONS**

#### **I. Background – The European Legal Framework**

The European Data Protection Directive 95/46/EC (“the Directive”) contains general provisions to ensure that data subjects are informed of their rights to data protection. These requirements are contained in the following articles:

- Article 6(1)(a), which requires that personal data be processed “fairly and lawfully”;<sup>1</sup>
- Article 10, which contains minimum information that must be provided to the data subject in cases when the data are collected directly from him.
- Article 11, which contains minimum information that must be provided to the data subject in cases when data about him are collected from a third party.
- Article 14, which contains a requirement to inform the data subject before personal data are disclosed to third parties

Overall the requirements in the Directive distinguish between two types of information. These are:

a) Essential information, namely– the identity of the controller and of his representative, if any, as well as the purpose of the data processing except where the data subject already has this information; and b) Possible “further information” including - the recipient of the data, the response obligation and the existence of access and rectification rights, in so far as such further information is necessary having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Furthermore, the Article 29 Working Party, (the WP) issued additional guidance in its Recommendation 2/2001 (WP 43, 17 May 2001) on certain minimum requirements for collecting personal data on-line in the EU. In its 2001 Recommendation, the WP gave important concrete indications on how the rules set out in the Directive should be applied to the most common processing tasks carried out via the Internet. It focused in particular on when, how and which information must be provided to the individual user and it was the first initiative to spell out on the European level a “minimum” set of obligations in a way that can be easily be followed by data controllers operating web sites. The present

---

<sup>1</sup> As explained by Recital No. 38 of the Directive, “...if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection...”.

opinion of the WP follows on from this Recommendation addressing the issue of more harmonised information to be provided in both on-line and of-line contexts.

## **II. The Current Implementation Framework**

The Commission's first report on the implementation of the Data Protection Directive (COM (2003) 265 final) looked at the implementation of the information provisions in the Directive. The report concluded that the *implementation of Articles 10 and 11 of the Directive showed a number of divergences. To some extent this is the result of incorrect implementation, for instance when a law stipulates that additional information must always be provided to the data subject, irrespective of the necessity test the Directive foresees, but also stems from divergent interpretation and practice by supervisory authorities.*

Indeed, the laws in the Member States vary very considerably with regard to the kinds of information that must be provided, the form in which it must be provided, and the time at which it must be provided. They also differ as to the kinds of additional information that may need to be provided to ensure a fair processing. Some Member States repeat the examples given in the Directive, others give somewhat different examples, and some give no examples at all. While some Member States stay quite close to the Directive's requirements, others have diverted considerably from them. More detailed information on national legislation is given in the **technical analysis** of the transposition of the 95/46 Directive in the Member States which accompanies the First Report on its implementation. ([http://europa.eu.int/comm/internal\\_market/privacy/lawreport/data-directive\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/lawreport/data-directive_en.htm))

These differences led the Commission to conclude that:

*"The present patchwork of varying and overlapping requirements as regards information that controllers have to provide to data subjects is unnecessarily burdensome for economic operators without adding to the level of protection."*

## **III. The work programme for a better implementation of the data protection directive (2003-2004)**

In order to ensure a more consistent approach to information requirements, the Commission included "*More harmonized information provisions*" as a specific action item (Action 6) of the work program for a better implementation of the directive. In this Action item, two parallel areas of work are identified:

1. Action to ensure consistency between national information requirements and the Directive:

*"In so far as information requirements placed on data controllers are inconsistent with the Directive, it is hoped that this can be remedied expeditiously through dialogue with the Member States and corrective legislative action by them."*

2. Article 29 Working Party collaboration in the search for a more uniform interpretation of Article 10

In the interests of moving forward on the second strand of action identified in Action 6 of the work program, the present opinion of the WP aims to establish a common approach for a pragmatic solution which should give a practical added value for the implementation of the general principles of the Directive towards developing more harmonized information provisions.

Such a pragmatic approach does not of course dispense the controllers from their present obligations to check their processing against the full range of requirements and conditions set up in the applicable national law in order to make it lawful.

#### **IV. The reasons to develop a more harmonized EU data protection information regime**

Four main reasons have been identified in support of more harmonized interpretation of Articles 10 and 11. These are:

##### **1. The need to facilitate compliance across the EU**

The Flash Eurobarometer 2003 survey of company practices clearly indicated that compliance with current information requirements is a problem. Responses from companies show that they do not always comply with data protection legislation by giving individuals the information to which they are legally entitled. For example only 37% of companies said they systematically provided data subjects with the identity of the data controller and only 46% said they always informed data subjects of the purposes for which the data would be used.

While the Eurobarometer survey suggested that larger companies are more likely to provide the relevant information than smaller ones, submissions to the review process on the directive stressed the difficulties even for larger companies seeking to comply with the current diversity of information requirements<sup>2</sup>.

##### **2. The need to improve citizen's awareness of data protection rights**

The results of the special Eurobarometer Data Protection survey highlighted the low level of citizen's awareness of data protection rights.

Only 42% of EU citizens are aware that those collecting personal information are obliged to provide individuals with certain information, such as at least their identity and the purpose of the data collection.

Simpler notices that facilitate citizen's awareness could help improve the current levels of understanding of data protection rights and responsibilities.

---

<sup>2</sup> See for example the views of the EPOF (European Privacy Officers Forum): [http://europa.eu.int/comm/internal\\_market/privacy/docs/lawreport/paper/epof\\_en.pdf](http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/epof_en.pdf) or the EU Committee of the American Chamber of Commerce: [http://europa.eu.int/comm/internal\\_market/privacy/docs/lawreport/paper/amcham\\_en.pdf](http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/amcham_en.pdf)

### **3. The need to present information with meaningful, and appropriate content to the data collection situation**

While the Directive makes a clear distinction between the basic information and possible “further information”, this distinction has not always been taken up in national interpretations. The result is that in some cases all national information requirements have to be given in all data protection collection situations. Such kind of interpretation does not reflect the spirit of Article 10 which makes a clear distinction between essential information and possible “further information” which should be provided only to the extent that is necessary to guarantee fair processing having regard to the specific circumstances in which the data are collected.

The requirement to provide extensive information in all data protection collection situations, irrespective of the necessity test that the Directive foresees, does not take into account the limitations of space or time in a number of data collection situations.

### **4. The need to improve the quality of data protection from the individuals’ perspective.**

On-line notices tend to be very long and contain legal terms and industry jargon. The value of such notices has been questioned in a study in 2002 by Consumers’ International entitled “Privacy@net, An International comparative study of consumer policy on the Internet”. This called for improved privacy information – and short, readable formats.<sup>3</sup>

## **V. Progress made so far – International Discussions**

The need for improved information on data protection has also been recognized at international level and important steps have already taken place at:

### **1. The 25<sup>th</sup> International Conference of Privacy and Data Protection Commissioners in Sydney.** This led to agreement on the Resolution contained in Annex 1. This resolution highlighted the need for greater consistency at the global level and stressed that notices must include:

- The information that is most important for individuals to know
- The information that individuals are most likely to want to know and
- The use of simple, unambiguous and direct language.

### **2. The workshop in Berlin in March 2004 that brought together public and private sector experts interested in building on the 25<sup>th</sup> International Conference Resolution.** These discussions led to agreement on a Memorandum

<sup>3</sup><http://www.consumersinternational.org/publications/searchdocument.asp?PubID=30&regionid=135&langid=1>

the full text of which is contained in Annex 2. This Memorandum endorsed the key strands of the 25<sup>th</sup> International Conference Resolution stressing the importance of comprehension, plain language, brevity and consistency. In addition, the memorandum explores :

- **How multi-layered notices could fit in a framework for compliance.**  
The memorandum suggests that information for data subjects could, where appropriate, be provided in a multi-layered format under which each layer should offer individuals the information needed to understand their position and make decisions. The memorandum also supported the idea of a framework for compliance. The idea is that in a multi-layered notice format the total format (i.e. all the layers taken together) must be compliant with relevant law, while each individual layer must communicate the information necessary for the individual to make an informed decision at that point in time.
- **Some of the key concepts to be included in short notices**  
It also supports the need to encourage consistent formats for notices.


3. **In September 2004 research was presented at the 26th International Conference of Data Protection and Privacy Commissioners in Wroclaw, Poland which demonstrated the need for easily understandable fair processing and privacy notices.** Notices need to be short, with limited categories of information and text, and must be in plain language. To assist comprehension and memory retention – and to promote more general awareness of data protection issues - they should preferably use a common format or standardized template. Layered notices, with full information available on request, can be used to communicate information available and ensure compliance with applicable law.

The Wroclaw conference was also told of research undertaken by MSN in Germany and Hong Kong to test the reaction of individuals towards actual layered notices. In both locations, despite differing concerns, individuals preferred the layered approach to conventional notices and saw them as more customer-centric privacy statements. The potential for the layered notice approach to be used internationally and in internet transactions was particularly noted.

## **VI. Towards a pragmatic solution - EU Information Notices**

At this stage, an important step would be to reach an agreement on the practical added value of developing information notices which would ensure a more harmonized interpretation of the Directive's relevant provisions across the European Union and that would meet simultaneously, the objectives of:

- Easier Compliance
- Improved awareness on data protection rights and responsibilities
- Enhanced quality of information on data protection



In the hope of encouraging a consistent approach to informing data subjects, a proposal is laid out below. This proposal is based on an analysis of the legal requirements set in the national data protection laws of the EU Members States and taking into account the Resolution of the 25<sup>th</sup> International Data Protection Commissioners Conference, the Berlin Memorandum which meets private sector's concerns, the needs of data subjects and, most importantly, the Directive 95/46/EC.

### Principles of Proposal


- **Support for the principle that information provided to data subjects, should use language and layout that is easy to understand.** Comprehension by data subjects is an important objective so they can make informed decisions and have the knowledge and understanding to influence the practices of data controllers and processors. In this context it is important to ensure that information is given in appropriate manner to people with particular needs (eg. children).
- **Support for the concept of a multi-layered format for data subject notices.** Multi-layered notices can help improve the quality of information on data protection received by focusing each layer on the information that the individual needs to understand their position and make decisions. Where communication space/time is limited, multi-layered formats can improve the readability of notices
- **Acceptance of short notices as legally acceptable within a multi-layered structure that, in its totality, offers compliance.** The sum total of the layers must meet specific national requirements, while each individual layer will be considered acceptable as long as the total remains compliant. In this way, businesses can use a consistent short EU data protection notice in consumer communications as long as they ensure that consumers can easily access information required under the national data protection regime.

### What information to be given in the EU Privacy Notices?

- Following the Directive a distinction can be made between two types of information to be given to the data subject upon collection of personal information. These are: Essential information **that should be provided in all circumstances** where data subject does not have this information already which includes the identity of the data controller and of his representative, if any, as well as the purpose of the data processing
- Further information which should be provided if it is necessary to guarantee fair processing **having regard to the specific circumstances in which the data are collected**

Going beyond this, there is also a third category of information which is nationally required and goes beyond the Directive's requirements, this includes information such as





the name or address of the data protection commissioner, details of the database and reference to local laws.

The Working Party in its present opinion endorses the principle that a fair processing notice does not need to be contained in a single document. Instead –so long as the sum total meets legal requirements - there could be up to three layers of information provided to individuals as follows:

### **Layer 1 – The short notice**

This must offer individuals the core information required under Article 10 of the Directive namely, the identity of the controller and the purposes of processing - except when individuals are already aware-and **any additional information which in view of the particular circumstances of the case must be provided beforehand to ensure a fair processing.** In addition, a clear indication must be given as to how the individual can access additional information.

Furthermore, there are some privacy-related situations in which it could be helpful to use even very short notices e.g. when the available space for information is extremely limited. So, very short notices could be developed for the display of mobile phones or other small devices. Sometimes even the use of pictograms can provide the necessary notice to the concerned persons. Obvious examples are the information on the installation of video-cameras or the use of RFIDs hidden in products.

Appendix 1 is an example of a short notice which could be adapted for use by a pan-European trading company.

### **Layer 2 – The condensed notice.**

Individuals must at all times be able to access a notice of information to include all relevant information required under the Directive. This includes, as appropriate:

- The name of the company
- The purpose of the data processing
- The recipients or categories of recipients of the data
- Whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply
- The possibility of transfer to third parties
- The right to access, to rectify and oppose
- Choices available to the individual.

In addition, a point of contact must be given for questions and information on redress mechanisms either within the company itself or details of the nearest data protection agency.

The condensed notice must be made available on-line as well as in hard copy via written or phone request. Data controllers are encouraged to present this notice in a table format that allows for ease of comparison. Appendix 2 is an example of a condensed notice.

Appendix 3 demonstrates how a condensed notice template could be used to give passengers on transatlantic flights the same information proposed for the Short Notice by the Article 29 Working Party in its Opinion 8/2004 of 30 September 2004. Both examples are designed with internet transactions in mind but can be easily readapted for off-line transactions.

**Layer 3 – The full notice.**

This layer must include all national legal requirements and specificities. It may be possible to include a full privacy statement with possible additional links to national contact information.

\* \* \* \* \*

The examples are well-suited for on-line activity, especially where a click through is provided from the short or condensed notice. They can easily be adapted for hard-copy format for off-line transactions, provided the individual is given a simple means (such as a free phone number) to obtain the required information.

**APPENDIXES**

- Appendix 1 example of a short notice
- Appendix 2 example of a condensed notice
- Appendix 3 example of a condensed notice for air travellers