



Unilever

UNILEVER 2004  
Data.

Agreed Joint Statement  
UEWC and Unilever on  
**protection of personal data**

# Contents

Agreed joint statement of UEWC and Unilever	3
Objectives and activities of the working party	5
Appendix 1	8
Appendix 1A	10
Appendix 1B	11
Appendix 2	12
Appendix 2A	13
Appendix 2B	14
Appendix 3	15

## Objectives and activities of the working party

The main objective was to examine the Unilever policy and ensure that it complies with both the European directive on the protection of personal data and is consistent with National legislation in all European Countries represented at the UEWC.

This objective has been achieved through a series of meetings. The initial meeting included a representative from the Unilever Legal department. At this meeting the policy and its implementation were discussed in detail and a number of written questions were submitted after this meeting for further clarification. This initial meeting was followed by a series of shorter meetings and electronic communications to clarify the finer points and to secure agreement that the policy as implemented is compliant with both national and EU legislation.

The main subject areas of concern from the employees and the results of the investigations can be summarised as follows:

### Understanding the Unilever policy and its extent of implementation.

The Unilever policy has been written for all Unilever companies with the intention that a single global policy will ensure that the highest standards are maintained. The company has indicated that it will expect all its subsidiaries to comply fully with the policy. Further it has indicated that before any information is transferred to a third party company, for example in the event of a proposed sale or transfer, the third party company will sign a confidentiality agreement.

Full details of the policy can be found on the Unilever corporate website (<http://legalnet.unilever.com>).

Establishing the amount and scope of data of a potentially sensitive nature that the company needs to transfer between countries.

The transfer of information in electronic form has become routine and it was essential that the group established the scale of the data transfer that falls under the remit of the legislation. Data held for panel tests and on consumer trials is always used in a coded format and is therefore not relevant to this investigation. The company holds personal information on all employees and some of this information could be regarded as

sensitive under some national legislation. Most of this data on individuals is held and used in a national context and therefore also falls outside the remit of the Unilever Works Council Agreement.

At the present time the only data that could be regarded as falling under the remit of the legislation is that held on the Universe data base. This is the personal data of all managers (WL2 and above) and a limited number of listed WL1 employees who may be being considered for promotion to WL2. The company indicated that this data is required to enable the sensible management of the company and individual career progressions particularly where individuals may be relocated between countries as part of their career development.

The employees had a concern that the disclosure of some personal data might unfairly influence or bias candidate selection for promotion. The introduction of the new "Open job posting" of all jobs (WL2 and above) means that individuals will supply their own data in support of their application. This should reduce the risk of personal data on file being used to influence selection. The company also uses password protection levels to limit access to the data held on individuals in the Universe database.

The working party is satisfied that these two practices are satisfactory and if applied in line with Unilever's general policies will ensure the appropriate level of privacy and fairness.

*The development of the National HR departments such as PeopleLink will improve management of data in line with National legislation but if these groups start to work in a trans-national format where a single HR centre manages more than one country we may need to revisit this topic.*

How to ensure that the level of sensitivity required by national legislation was not put at risk by the policy because of differences in the interpretation of the definition of what is sensitive.

This was a difficult issue for the working party as we did not have the detailed knowledge of all the National policies. It was therefore agreed that each National Personnel Manager would be requested to discuss the

Unilever Policy with their local departments concerned. Their confirmation that the policy is in line with their own national legislation will be accepted by the working party.

The attached appendices show both the managers responsible for data protection in each country and their indication that the Unilever policy is in line with their national legislation.

Establishing the scope of the Unilever directive as applied to countries outside the EU which are not covered by the requirements of the EU directive.

There were two concerns in this context. The first is that local companies may feel more bound by national legislation than Unilever policy and in some countries there are no statutory restrictions on electronic communications.

The working party has been assured that the policy will be applied in all Unilever companies.

The second concern was that in some countries, notably the USA, information is assumed to be open access unless marked as private. The use of "cookies" was used as an example. In Europe the assumption is that data is private unless marked as open access. The concern was therefore that by default personal information could become open access if located on for example an American server.

The company has given the working party the assurance that all data will be treated as confidential with restricted access irrespective of its location within the company.

Again the policy requires that before information is passed to third parties, as in the event of a sale of business, the recipient also has to sign a confidentiality agreement.

Who will be responsible for ensuring the policy is implemented?

The Unilever Policy and its implementation will be the responsibility of national managers but in each country a Data Protection Officer will be appointed and made responsible for the maintenance of the integrity and use of the database at national level.

The Unilever Audit team as part of their normal practice will also audit the process and management have agreed to report back to the UEWC the outcome of any such audits as and when they take place.

#### Supplementary information

Appendix 1	Letter with answers to specific questions (Joba van den Berg, 27 November 2002)
Appendix 1A	Request process
Appendix 1B	Request form
Appendix 2	Letter with answers to outstanding questions (18 March 2003)
Appendix 2A	Compliance List
Appendix 2B	Unilever Corporate Privacy Policy
Appendix 3	Data Protection Officers as of February 2004

# Appendices

# Appendix 1

European Works Council Working Party  
Mr. Sj. van 't Wout  
Mr. D. Ward  
Mr. A. Magne  
Mrs. S. Piel

27 November 2002

Dear Sirs/Madam,

In reference to your letter dated September 26, 2002 regarding the European status on Protection of Personal Data we would respond as follows.

## **Compliance**

As you will know the Personal Data legalisation is based on the 1995 European Directive which had to be implemented before October 24, 1998 but was delayed in many countries. A European directive has to be implemented into national legislation as it has no direct effect.

Unilever disseminated to all countries their general policy, in the form of a Unilever Privacy Policy Guide plus an implementation letter. You received copies of these documents. This Policy Guide has to be implemented in each country taking into account national legislation.

To check if all countries involved in the EWC have implemented the policy we have sent a request to inform us about their date of implementation and their affirmation of compliance. When we have received the answers we will send you an overview.

## **CEE countries**

Firstly, all CEE countries received the general Unilever policy. Secondly the CEE countries have to comply in phases with European legislation before they can be accepted as full member. Hungary and Czech Republic are within Unilever seen as regulated countries and had to comply fully with the Unilever policy ultimately October 23, 2001. The other CEE countries are non-regulated countries which means they have to comply fully with the Enabling Instructions of which you received a copy.

## **Protection officers**

We will provide you with a list of the key data protection officers (appendix 3) as far as currently available. We will suggest National Managements to publish the names of the responsible person(s) in their country.

## **Appendices E and J of the Unilever Policy**

### **1. The database fields:**

Please note that names of children and marital status are not seen as confidential information. Protected fields which need separate permission are work level, listing and salary information. Access rights are controlled per user by Corporate HR; the access procedure requires approval from an HR director or business group HR department to give access to a new user, and also which data they can see. Please find as appendices 1A and 1B copies of the request process and of the request form.

The company ensures compliance by controlling access rights and passwords.

2. To third parties only those fields are disclosed which are absolutely necessary to inform e.g. a potential buyer. The latter has to sign a confidentiality agreement.
3. None of the fields require special permission of the individual as all disclosures are within the aim of the data processing.

### **Breaches of the company policy**

In case of breaches proper measures will be taken.

### **Infrastructure**

Regarding the migration of IT infrastructure: the PeopleSoft database will be migrated to the United States. The Company is not just looking at UK legislation, EU legislation is followed as well as local legislation overseas. With regard to the EU legislation the company has ensured all countries with access to comply at minimum with the EU legislation.

### **UK website**

The information on the UK website is a "Guidance" for the Unilever Global Privacy Policy. The Policy does require that local laws must be complied with. The appendices are only examples intended to be helpful and are not supposed to be copied without proper consideration. As you will know a European Directive requires adaptation to national legislation. So, if certain issues are nationally forbidden this have to be taken into account. For example: in NL union membership is not mentioned.

If you have any further questions, please do not hesitate to contact me.

With kind regards,

Joba van den Berg-Jansen

CC: W. Selman

## Appendix 1A

### Access Request Process (update August 2004)

1. There is one standard global process that will not be dependent on from where/whom the request originates as to the most appropriate process to follow. In the main, people should channel their request through their Service Center/PeopleLink (HR IS Business Support Group).
2. Requests from Corporate Centre Departments should be channelled through the Service Center/PeopleLink (HRIS Business Support).
3. User/the employee/BU HR to channel request through the appropriate route to obtain agreement and forward agreed request together with relevant access level to HRIS Business Support (within PeopleLink).  
Support.PeopleSoft@unilever.com.
4. HR IS Business Support creates a ticket in the customer service request system (STAT) requesting to set up User ID and Password.
5. HRMS - ET receives STAT ticket. The appropriate roles and/or permission lists are assigned to the user ID, based on the approved System Access Request form. An e-mail is sent to PeopleLink and the user when the request is complete, providing the user's ID and password, where necessary.

### Password Resets

⌚ If Users get locked out, passwords can be reset by HR IS Business Support:

Email Account(NL): ✉ Support.PeopleSoft@unilever.com

HelpDesk Phone(NL): ☎ +31 (0) 10 460.8411

HRMS-ET-Email-Account: ✉ Competence.Centre@unilever.com



# Appendix 1B

Request for new User

Date:

Name:

Job Title:

Company:

Authorised by HR Director (pls. print name):

Name of the current user (if you are replacing someone)	Brief description of which data will be used. (Pls. specify which kind of data you will use; e.g.all records of company X plus expats abroad).	Aztec or NT user ID	Restriction required re. access to List, PP, and Salary information

## Appendix 2

European Works Council  
Working Party Protection Personal Data

18 March 2003

Dear Sirs/Madam,

In the December 2002 meeting of the Co-ordination Committee of the European Works Council, there were still some questions left re the Protection of Personal Data, which we would appreciate to answer as follows:

### 1. Compliance list

A compliance list is enclosed as appendix 2A. Please note that Ireland and Portugal still have to confirm; we will inform you as soon as possible.

### 2. Sensitive information when applying for a job

The Open Job Posting system does not request information on e.g. marital status or children. The information given before a job offer is made is mainly dependent on the person himself. See <http://central.unilever.com/foundation/exec> for the required information in case of OJP.

Please note that from a legal point "confidential" is not a used term. For example: the Dutch Privacy Legislation refers to "special" (as sensitive) information which is limited to information on health, criminal records, religion, political choice, sexual lifestyle and union membership. In some countries ethnic information is seen as "special".

Please note as well that all data collected can only be collected for a well-defined and justified purpose:

### 3. Audit of policies

All listed Unilever Policies are annually audited by the Positive Assurance Facilitation and so are the Privacy Policies. Moreover, Corporate Audit takes annually a "theme" audit in which special attention is paid to (a) certain theme(s).

### 4. Privacy Statement

The Privacy Statement (see appendix 2B) is also applicable for the USA.

If you have any further questions, please do not hesitate to contact me.

With kind regards,

Joba van den Berg-Jansen

# Appendix 2A

## Summary of responses to request confirming national compliance

### Compliance

Country	Compliance	EU legislation implementation	Implementation Unilever Policy
Belgium	Yes	2002	2002
Czech Republic	Yes	01 February 2002	since April 2002
Denmark	Yes	26 May 2000	since June 2002
France	Yes	2002	1978
Germany	Yes	23 May 2001	since August 2001
Greece	Yes	1997	since December 2001
Hungary	Yes	27 June 2002	27 June 2002
Italy	Yes	08 May 1997	since October 2001
Poland	Yes	1 May 2004	Confirmed October 2003
Spain	Yes	since 2000	since February 2002
Sweden	Yes	2002	since 22 February 02
The Netherlands	Yes	since September 2001	since July 2002
UK	Yes	23 October 2001	Confirmed March 2001
Austria	Yes	2002	2002
Finland	Yes	2002	2002
Ireland	Yes	2002	Confirmed September 2003
Portugal	Yes	2002	Confirmed September 2003
Switzerland	Yes	2002	2002

March 18, 2003 Updated January 2004

## Appendix 2B

### Unilever Corporate Privacy Policy

This Policy governs Unilever's practice with regard to the processing of personal data concerning consumers, employees and other persons.

#### General

1. Personal data must only be used in conformity with applicable laws and regulations and any Instructions prescribed by Unilever.
2. In the holding and processing of personal data relating to consumers, employees and others we will be guided by the following principles:
  - personal data must be collected fairly;
  - individuals must give their "agreement" to the collection and use of their data;
  - the data collected must not be excessive given the purposes for which it is required and it must be kept accurate and up-to-date;
  - appropriate security measures need to be taken to prevent unauthorised use and accidental loss or damage; and
  - we must assist individuals with enquiries they have about their data which we hold and must comply with any requests that data is not used for direct marketing purposes.
3. Personal data must not be used in any way that might bring any Unilever Group companies into disrepute.
4. Where there is any conflict with applicable laws and regulations and Instructions prescribed by Unilever, the laws/regulations must be followed and the relevant person in a Business Group/Organisational Unit and the Legal Group should be notified.

#### Implementation Responsibility

5. The General Counsel has authority and is responsible for issuing Instructions to implement this Policy.
6. It is the responsibility of the appropriate President/Head of each Business Group/Organisational Unit to ensure that all relevant Unilever employees are made aware of this Policy and the Instructions and that the Policy and Instructions are implemented throughout the

Business Groups/Organisational Units. Each Business Group and Organisational Unit is responsible for setting up procedures for monitoring and enforcing compliance with this Policy and the Instructions. Business Groups, Organisational Units, National Managements and Company Chairmen must co-operate with this.

7. In the first instance enquiries on this Policy must be made to the relevant person responsible for this Policy in each Company, Organisational Unit or local legal department. Questions regarding interpretation, revision and update of this Policy must be directed to local legal departments and where relevant to the Legal Group, Corporate Centre, London. Legal Group, London remains the Policy owner.

July 2001

# Appendix 3

## Regional DPO status

01/11/02

### Data Privacy Policy status overview – February 2004

Sub-region: D.A.CH.		
Operating Company	Name of DPO for HR	Name of DPO for M/S
<b>HPCE</b>		
Germany	Johannes Baumgartner	Laurence Besnard-Royes
Austria	Helmut Gattinger	Cornelia Eichner
Switzerland	Werner Koller	Bernd Michahellis
<b>ICFE</b>		
Germany (Langnese)	Johannes Baumgartner	Timo Kramp
Germany (FFI)	Johannes Baumgartner	N/A
Austria (Eskimo-Iglo)	Helmut Gattinger	Sabine Schlechta
Switzerland (Pierrot-Lusso)	Philip Mathys	Philip Mathys
<b>UBFE</b>		
Germany	Johannes Baumgartner	Foodsolutions: Erik Fischer Retail: Imke Grassau-Zetsche
Austria	Hans Stieger	Rudolf Obermair
Switzerland	Urs Beck	Goris Verburg

Sub-region: Italy – Greece		
Operating Company	Name of DPO for HR	Name of DPO for M/S
<b>HPCE</b>		
Lever Fabergè Italy	Rinaldo Martelli	Michele Martinenghi
Greece	Vassiliki Koutsospyrou	Vrahiola Katerina (Marketing) Theodoros Kourtsounis (Sales)
<b>ICFE</b>		
Sagit Italy	Svevo Valentinis	Antonio De Paolis
<b>UBFE</b>		
Unilever Bestfoods Italy	Franco Gaudino	Marco Toso
UBF/ICFE Greece	Yiannis Hadjis	Paclos Limberakos
Israel	Stan Freeman	Stan Freeman
Turkey (Algida)	Cezmi Ozkunt	Deniz Akturk Erdem

Data Privacy Policy status overview – February 2004

Sub-region: Nordic

Operating Company	Name of DPO for HR	Name of DPO for M/S
<b>HPCE</b>		
Lever Fabergé Denmark	Alice Soerensen	Heidi Borgmann
Lever Fabergé Sweden	Bjoern Stalnacke Sylvia Buddenbaum	Sylvia Buddenbaum
Lever Fabergé Finland	Jaana Palmunoksa	Oskari Rovamo
HPC Norway (NON Unilever company)		
<b>ICFE</b>		
Frisko Denmark	Alice Soerensen	Jesper Bernhoft
GB Glace Sweden	Bjoern Stalnacke	Anna Hallov
<b>UBFE</b>		
UBF Sweden-Denmark	B. Stalnacke/ H.O.Petterson - S Alice Soerensen - DK	Eva Fried
UBF Finland	Jaana Palmunoksa	Oskari Rovamo

Sub-region: France

Operating Company	Name of DPO for HR	Name of DPO for M/S
<b>HPCE</b>		
Lever Fabergé France	Sacha Bulyk	Frederique Villiard
<b>ICFE</b>		
Cogesal - Miko	Christine Michau	Stanislas Bresson
<b>UBFE</b>		
UBF France	Jean Roiesnel	Denis Reynaud-Lacroze
National Management	Dominique Nioré	N/A

Data Privacy Policy status overview – February 2004

Sub-region: Benelux		
Operating Company	Name of DPO for HR	Name of DPO for M/S
<b>HPCE</b>		
BG HPCE	Willy van Rillaer	Catherine Thieltgen
LF Belgium	Willy van Rillaer	Catherine Thieltgen
LF Netherlands	Joke Hoekveld	Harry Dekker
<b>ICFE</b>		
Iglo-Ola	Willy van Rillaer	Catherine Thieltgen
IgloMora	Maarten Smits	Stef Gans
<b>UBFE</b>		
UBF Belgium	Willy van Rillaer	Catherine Thieltgen
UBF Netherlands	Monique vd Mijle	Aleid Auwerda, Martijn Beijer, Winfried de Ruijter, Piet-Hein Speel, Sander van Pelt, Danielle vd Broek
R & D Vlaardingen	Cees Hoekman	N/A
PeopleLink	Jille Tabak	
corporate Centre	Ellen de Grijs	

Sub-region: Iberia		
Operating Company	Name of DPO for HR	Name of DPO for M/S
<b>HPCE</b>		
LeverFab.Spain	Ricardo Bacchini	Ignacio Domínguez/Juan-Manuel Vergara
LeverFab.Portugal	Victor Vale	Pedro Casquinha
<b>ICFE</b>		
FRIGO Spain	José Antonio Quintana	Raquel Sugranyes
IGLO Portugal	Victor Vale	Pedro Casquinha
<b>UBFE</b>		
AGRA Spain	Rosa Araujo (Barcelona Site) Javier Sanchez (Bilbao site)	Lina Piedrahita / Igor Unzalu (Retail) John Harrel (Food Solutions)
UBF FIMA Portugal	Victor Vale	Pedro Cruz
National Mgmt. Spain	Rafael Burgos	N/A

Data Privacy Policy status overview – February 2004

Sub-region: CEE

Operating Company	Name of DPO for HR	Name of DPO for M/S
HPCE USCE/U South Central Europe/	Rodica Barascu	Gabriel Stanciu
ICFE UBFE		
Poland	Barbara Duniec	Agata Lodzinska
Czech and Slovak Republics	Stepanka Brdova	Stepanka Brdova
UL Hungary/Croatia/Slovenia	Scilla Szabo	Andras Szirbek Csilla Fabian Balazs Feher Marton Pataki
Baltic's Russia & Ukraine	Sanita Silina Natalia Karaseva	Alina Suste Galina Karaseva

Sub-region: UK and Ireland

Operating Company	Name of DPO for HR	Name of DPO for M/S
HPCE		
LF UK Leeds Factory Port Sunlight	Lesley Taylor Nicola Taylor Steve Trubridge	Dave Saunders N/A N/A
LF Ireland Research Port Sunlight	Martin Smith (ISO) TBA	Martin Smith (ISO) N/A
ICFE		
BEW UBF Ireland	Gavin Mitchell Seamus Dolan	Nicki Hickson Barry Thornton
UBFE		
UB UK Research Colworth PeopleLink Corporate Centre	Marcus Tofts Colin Williams Sarah Saville Dawn Bartrum	Marcus Tofts N/A