Enhancing the efficiency of alerting systems through personalized, culturally sensitive multi-channel communication

Project No. 261699

Deliverable D7.1.

"Report on legal data protection and privacy requirements"

Contributing Partner(s):

Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (FHSS)

Introduction

This report presents an overview of the relevant legal framework with regard to data protection and privacy issues of the Opti-Alert project. The report is structured as follows:

(1) In the following section, an overview of relevant EU directives and regulations as well as relevant national data protection laws in the countries under analysis will be presented.

(2) Thereafter, the European data protection and privacy legislation and its relevance for the project work within Opti-Alert is discussed. This discussion focuses both on the basic research to be conducted in the project (personal interviews, questionnaire-based studies) as well as the technical implementation of Opti-Alert services in the demonstrator.

(3) Finally, the report concludes with an analysis of relevant national norms to be observed in the project work, that is, the data protection laws of Germany, France, Italy, Sweden, Austria, the Netherlands, and Hungary.

The legal framework: an overview

The European Union has a long-standing policy to provide legal safeguards for the protection of personal data. The legal framework established by the European Union to achieve this goal currently consists of the following key elements:[1,2]

- the Charter of Fundamental Rights of the European Union[3];
- Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[4]; and
- Directive 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications[5].

In order to translate these directives into national legislation (and to possibly establish regulations beyond the *acquis commun*), the countries affected by Opti-Alert have adopted the following data protection laws:[6]

---

[1] Manolescu, D.: Data protection as a fundamental right. In: effectius newsletter, Issue 5, 2010.

[2] Note that the European Data Retention Directive (2006/24/EC) is not relevant for the Opti-Alert project because none of the partners in the project operates a service directly covered by this directive. Cooperation partners outside the Opti-Alert project may, however, be affected (e.g., external SMS and E-Mail service providers).

[3] Official Journal of the European Communities C 364, 18/12/2000, pp. 1-21. (http://www.europarl.europa.eu/charter/pdf/text_en.pdf)

[4] Official Journalof the European Communities L 281 , 23/11/1995,.pp. 31-50. (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML)

[5] Official Journalof the European Communities L 201 , 31/07/2002, pp. 37-47. (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF)

- Austria: Federal Act Concerning the Protection of Personal Data ("Datenschutz-gesetz", DSG 2000[7])
- France: Act no. 78-16 of 6 january 1978 on Data Processing, Data Files and Individual Liverties («Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés»[8]), modified by the «Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés».[9]
- Germany : Federal Data Protection Law ("Bundesdatenschutzgsetz", BDSG)[10]
- Hungary: Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest [11], Article 59 of the Constitution of the Republic of Hungary[12], Act CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing[13]
- Italy: Personal Data Protection Code – Legislative decree no. 196 of 30 June 2003 ("Decreto Legislativo 30 giugno 2003, n. 196 codice in materia di protezione dei dati personali"[14])
- The Netherlands: Personal Data Protection Act ("Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens"[15])
- Sweden: Personal Data Act 1998:204 ("Personuppgiftslagen"[16]), including related decrees ("Personuppgiftsförordning"[17])

---

[6] NYMITY: Primary Data Protection Laws in the European Union and the EFTA. http://www.privacybydesign.ca/content/uploads/2010/03/NYMITY-EU_map.pdf

[7] Full text: http://www.dsk.gv.at/DocView.axd?CobId=40904 , in English: http://www.dsk.gv.at/DocView.axd?CobId=41936 (unofficial translation)

[8] Full text (in French): http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624

[9] Full text (in French): http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676&dateTexte

[10] Full text (in German): http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf

[11] Full text (translation into English): http://abiweb.obh.hu/adatved/indexek/AVTV-EN.htm

[12] Full text (translation into English): http://www.ceecprivacy.org/main.php?s=2&k=hungary

[13] Full text (translation into English): http://www.ceecprivacy.org/htm/dmtv-en.htm

[14] Original text: http://www.parlamento.it/parlam/leggi/deleghe/03196dl.htm, Translation into English: http://www.privacy.it/privacycode-en.html

[15] Full text (in Dutch): http://wetten.overheid.nl/BWBR0011468/geldigheidsdatum_21-03-2011, Unofficial translation into English: http://www.dutchdpa.nl/downloads_wetten/wbp.pdf

The overview of the legal framework presented in this section refers to applicable law as of March 23rd, 2011. Please note that the field of data protection and privacy law is still evolving, so that the reader is strongly advised to check the validity and current content of the different laws and regulations when consulting this document in the future.

The European framework

Charter of Fundamental Rights of the European Union

In Article 8, the Charter of Fundamental Rights of the European Union stipulates that "Everyone has the right to the protection of personal data concerning him or her" (Art. 8 No. 1). This includes the right to fair processing of personal data for specified purposes (only). Processing of personal data either requires consent of the person in question or an explicit legal basis for doing so. Notwithstanding the reason why the personal data is collected and processed, everyone has the right to access the data that has been collected on him / her and to have it rectified in case of errors (Art. 8 No. 2).

Conclusion for the Opti-Alert project:

Unless there is a separate specific legal basis for the processing of personal data in Opti-Alert, storing and using such data requires the consent of the person to whom the data is related. Project partners who collect and store personal data must define a procedure to allow individuals to access the data collected on him / her. The procedure also has to include rules on how to deal with complaints, i.e. requests for rectification.

Directive 95/46/EC

Directive 95/46/EC provides the general framework for the handling and processing of personal data in the European Union, **as long as these data are processed wholly or partly by automatic means** or **form part of a filing system** or **are intended to form part of a filing system** (Article 3 No. 1). Filing system in this respect refers to "any structured set of personal data which are accessible according to specific criteria", regardless of the type of criteria used to access them (Article 2 (c)).

Directive 95/46/EC does not apply to "processing operations concerning public security, defence, state security... and the activities of the state in areas of criminal law" (Article 3 No. 2).

Collection and further processing of personal data for scientific purposes is licit (Article 6 No. 1 (b)) as long as it is **adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed** (Article 6 No. 1 (c)).

Legitimate processing of personal data can be ensured if **the data subject has unambiguously given his consent** (Article 7 (a)) or **processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority** (Article 7 (e)).

---

[16] Full text (in Swedish): http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=1998:204, translation into English: http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf

[17] Full text (in Swedish): http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=1998:1191:

It is prohibited to process personal data that reveals **racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life** (Article 8 No. 1). Again, if the data subject gives explicit consent processing is allowed (Artikel 8 No. 2 (a)) as long as national laws do not prohibit this explicitly.

As of Article 10 the data subject has the rights to get informed (a) who is collecting his data, (b) what is the purpose of processing the data intended for, (c) who is the recipient of the data. The data subject has the right of access and to rectify the data concerning him. Fair processing of the collected data has to be guaranteed.

Specifically for the operation of systems where data is collected without a data subjects notice (e.g. location data) Article 11 needs to be respected. In that case the controller has to inform the data subject to whom and which collected data may be disclosed to a third party no later than the time when this data is disclosed the first time.

As already mentioned the data subject has the right to obtain his collected data (Article 12). It hast to be guaranteed that the data can be obtained **without constraint at reasonable intervals and without excessive delay or expense** (Article 12 (a)).

According to Article 17 of this Directive the controller of the collected data **must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access** (Article 17 No. 1). This is especially important when data is transmitted over a network. **Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.** If the processing of the data is carried out by a third-party that is not the controller of the data, a contract or binding legal act has to be set up to ensure compliance with aforementioned measures.

The controller of the collected data has to notify the supervisory authority before carrying out any wholly or partly automatic processing operation (Article 18 No. 1). Simplification or exemption from this notification can be granted if e.g. the controller appoints a personal data protection official, **thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations** (Article 18 No. 2). It may be stipulated **that certain or all non-automatic processing operations involving personal data shall be notified** (Article 18 No. 5).

Article 19 No. 1 specifies the information that has to be notified at least: **(a) name and address of the controller and of his representative, if any; (b) the purpose or purposes of processing; (c) description of the category or categories of data subject and the data or categories of data relating to them; (d) recipients or categories of recipients to whom the data might be disclosed; (e) proposed transfers of data to third countries; (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing**. Procedures need to be specified how changes affecting this information are notified to the supervisory authority.

Conclusion for the Opti-Alert project:

Although some alerting activities carried out by the Opti-Alert demonstrator may be categorized as "processing operations concerning public security" etc. and may therefore be exempt from the provisions of the directive, the Opti-Alert system as a whole will have to take Directive 95/46/EC into consideration.

During the activities of data collection for basic research (primarily survey data and its processing) specials means have to be addressed: Interviewers have to take care that data is collected as sparsely as possible. Especially, contact data (e.g. phone and e-mail) should only be accessible to the interviewers if further interaction with the respondents is necessary. For demographic evaluation address data should be generalized.

Due to the nature of conducting interviews, the respondent will know what personal information is collected. The data subject gives an explicit opt-in for collecting this data when taking part in that survey. Therefore fulfilment of Article 7 of the Directive is guaranteed. Nevertheless, proper mechanisms have to be installed so that a respondent has the possibility to obtain the collected data to a later point in time.

If web portals are used to conduct some of these surveys and third-party services are used, as of Article 17 these service providers have to be contracted to fulfil all legal requirements concerning the privacy of the collected data. Other project members apart from the interviewers shall not get in contact with the unprocessed data of the respondents. It shall be documented who (and in which role) will get access to the personal data.

Project partners have to use secure means to distribute and communicate collected data among each other. Hence, communication has to be encrypted for that specific kind of data.

Besides the basic research special means have to be installed to safeguard the operation of the demonstrators: As automatic data (e.g. location data) may be stored in the devices or on servers, the subscriber of the service need to be informed on the terms and conditions of the service. By using the service the subscriber gives consent to collect and process the personal data, as demographic data will be used to automatically generate customized warning messages for the subscriber. Nevertheless, only the minimum data to operate the service should be collected (i.e. for a free service no payment information must be collected etc.).

To safeguard that all legal regulations are met the project should install a personal data protection official.

Regulation of communication of collected data to third-party countries does not apply as all project members are situated in countries belonging to the EU.

Directive 2002/58/EC

Directive 2002/58/EC provides the framework for the processing of personal data and privacy protection in electronic communications. One major concern that is addressed in this directive is the usage of location and traffic data that is used apart from billing purposes. Therefore, distinctions between communications networks providers and value added services that are publicly available are made.

The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented (Article 4 No. 1).

It shall be ensured **that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment** (e.g. mobile handsets) **of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC** …, **and is offered the right to refuse such processing by the data controller** … (Article 5 No. 3).

Especially **traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication** … (Article 6 No. 1). **Processing the traffic data** … **must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services** …, **and must be restricted to what is necessary for the purposes of such activities** (Article 6 No. 5).

Where location data other than traffic data … **can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers** … **of the type of location data other than traffic data which will be processed, of the purpose and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time** (Article 9 No. 1). **Processing of location data** … **must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service** … (Article 9 No. 3).

Conclusion for the Opti-Alert project:

As this Directive distinguishes communications networks providers and/or value added services explicitly (e.g. e*Message participates in both roles, SMS or push notifications are provided via value added services) this has to be considered in the operation of the demonstrator.

As already mentioned for Directive 95/46/EC subscribers give their consent to collect personal data by using the service explicitly (to be clearly outlined and unambiguously stated in the terms and conditions of the service). Again, data to be collected must be as sparse as necessary to ensure service's operation. Location data may be used to generate personalised messages for the subscriber. If this location data needs to be stored on servers, the information should be deleted (or at least anonymised) as soon as possible to prohibit unauthorized tracking of the subscriber.

Taking e*Message's system as an example, no tracking data is stored at the service provider because the system is broadcasting warning messages. It is the terminal equipment itself which decides by specific identifiers if the message is targeted for that subscriber (point to multipoint communication via data broadcast).

Even if the service provider is able to associate terminal equipment with a subscriber, location data of the subscriber is not disclosed to the service provider.

National peculiarities in the participating countries

Austria

The Austrian regulation specifies in §17 a passage so that applications which collect personal data are subject to registration. Nevertheless there can be exceptions of this rule if the collected data is regarded as a "standard application". The according standard application data (and its max. allowed storage time) is specified in "Gesamte Rechtsvorschrift für Standard- und Muster-Verordnung 2004, Fassung vom 28.04.2011"[18].

Austrian partners are thus required to register their data processing activities unless they can prove that the data to be processed is included in the aforementioned list of "standard application data". Concerning the processing of data for scientific purposes only, Austria opted to implement an exception of this rule as long as personal data is only used to generate un-personal meta-information (§46 (1)). In this particular case the personal data used either has to be publicly accessible, has to be legally acquired for a different purpose or is only indirectly related to an individual. In all other cases data subjects have to agree with the processing, the processing has to be permitted by the Austrian data protection commission or has to be explicitly permitted by law (§46 (2)).

France

The law in France stipulates that personal data used for the (secondary) purpose of statistical, scientific or historical research may not be ***used to take decisions*** in respect of the data subjects (Korff 2002[19], please note that the the study by Korff only incorporates "planned" amendments of French data protection law and not necessarily the final text as implemented in law n°2004-801). The same study by Korff also concludes that French law "contains a special provision allowing the use of "**cookies**" only if the controller has first informed the user (i.e. a visitor to his website) of the ***purposes of the processing*** and of the ***means available to oppose*** the

[18] Full text (in German): http://www.dsk.gv.at/DocView.axd?CobId=30704

[19] Korff, D.: EC study on implementation of data protection directive – comparative summary of national laws. Essex: University of Essex, 2002.

processing, in "***clear and comprehensive terms***". The webhost may, moreover, not make the acceptance of a "cookie" a ***condition*** for access to the service in question." (p. 101)

The latter provisions may be relevant if the Opti-Alert plans to use online questionnaires for surveys or provides registration to the Opti-Alert demonstrator via a web site.

Germany

The Bundesdatenschutzgesetz (BDSG) (last authoritative version from 14.08.2009) is already aligned to the Directive 95/46/EC. Therefore this Directive is referenced when cross-bordered collection and communication of personal data is discussed.

Hungary

Please note that, in accordance with Art. 3 (2) a) of Act No. LXIII of 1992, special categories of personal data may require **consent in writing (!)** by data subjects in order to allow for processing of these data.

This may pose an obstacle for conducting computer-assisted telephone interviews in the framework of Opti-Alert. Research partners planning such interviews in Hungary are strongly advised to verify if the data which they plan to collect and process require written consent by the data subjects. If so, they need to contact the data subjects before the telephone interviews in order to obtain the required permission in writing.

Information requests by data subjects on the processing of their personal data must be answered **in writing** and within 30 days after the request has been made (Art.12 (2)).

Hungary has also opted to implement specific provisions concerning the use of name and address information in research (Act CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing). These provisions are in some cases less stringent than the general provisions, and allow for a transfer of address data from, for example, address registries (Section 3 (1) d) unless the data subject has objected to such processing (opt-out). The same exemption is valid for such data received from organisations "in the same line of business" if the data subject has been informed about the planned transfer and did not object (Section 3 (1) c). On an opt-in basis, the same exemption holds true for data collected in data registries with the purpose to be published (e.g., telephone books, Section 3 (1) a).

If research partners in the Opti-Alert project plan to use these exemptions provided by Act CXIX of 1995, they are obliged (Section 7 (1) a) –f)) to specify a data processing plan comprising

- the entitlement to conduct research,
- the objective of the research,
- the source and sphere of personal data to be used,
- the process of data use,

- guarantees for practical enforcement of the subject party's rights (including the right to opt-out at any time), and
- the technical and organisational measures taken for data protection.

Additionally, research partners are advised to verify if the planned data processing might be negatively perceived by data subjects concerned. It should, under all circumstances, be avoided that such processing negatively affects the reputation of Opti-Alert.

Furthermore, it is of utmost importance that all permissions granted by data subjects as well as data processing plans are properly documented and kept, as, in case of dispute, it is the duty of the data controller to prove that the processing have complied with provisions of law (Art. 17 (2) of Act No. LXIII of 1992).

Italy

In Italy, codes of conduct and professional practice for specific sectors can be published in the Official Journal of the Italian Republic and then become legally binding for data controllers in this sector. Therefore, Italian partners need to verify if such codes exist for their own sector. In particular the "CODE OF CONDUCT AND PROFESSIONAL PRACTICE APPLYING TO THE PROCESSING OF PERSONAL DATA FOR STATISTICAL AND SCIENTIFIC RESEARCH PURPOSES WITHIN THE FRAMEWORK OF THE NATIONAL STATISTICAL SYSTEM" may be relevant for activities in the Opti-Alert project.

The Netherlands

In addition to EU standard regulations the WBP also prohibits the processing of personal data concerning a person's criminal behaviour, or unlawful or objectionable conduct connected with a ban imposed with regard to such conduct (Article 16).

The prohibition on processing personal data concerning a person's race … does not apply where the processing is carried out: (b) for the purpose of assigning a preferential status to persons from a particular ethnic or cultural minority group with a view to eradicating or reducing actual inequalities, provided that (Article 18 in WBP). With regard to Opti-Alert this may allow the processing of racial data in the Netherlands without consent of the individual with the purpose to improve the impacts of alerts to ethnic minorities which currently suffer from disadvantages in disaster situations.

Sweden

If a personal data representative has been appointed by the controller and the data subject have given consent to the intended processing of their undiscriminating[20] data, the processing does not need prior approval by the Data Inspection Board.

[20] personal data concerning hereditary disposition derived from genetic investigation

Regulatory bodies[21]

The following regulatory bodies have been established in the countries affected by research activities in the Opti-Alert project and may be contacted for permissions and legal updates.

Austria

Österreichische Datenschutzkommission
Frau Dr. Eva Souhrada-Kirchmayer
Hohenstaufengasse 3
A - 1010 Wien
Phone: + 43 1 531 15 2525
Fax: + 43 1 531 15 2690
E-Mail: dsk@dsk.gv.at

France

Commission Nationale de l'Informatique et des Libertés (CNIL)
Président Alex Türk
8 rue Vivienne
CS 30223
F - 75083 Paris cedex 02
Phone: + 33 (0)1 53 73 22 22
Fax: + 33 (0)1 53 73 22 00
E-Mail: webmaster@cnil.fr

Germany

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Husarenstraße 30
D-53117 Bonn
Phone: +49 (0)22899-7799-0
Fax: +49 (0)22899-7799-550
E-Mail: poststelle@bfdi.bund.de

Please note that each state in Germany has its own regional data protection officer, the contact details of these can be retrieved from http://www.bfdi.bund.de/DE/AnschriftenUndLinks/Landesdatenschutzbeauftragte/Landesdatenschutzbeauftragte_node.html if needed.

[21] Contact details for regulatory bodies in participating countries have been retrieved from the website of the German Federal Data Protection Officer, http://www.bfdi.bund.de/DE/AnschriftenUndLinks/AuslaendischeDatenschutzbeauftragte/AuslaendischeDS_node.html (as of April 30th, 2011)

Hungary

Parliamentary Commissioner for Data Protection and Freedom of Information
Dr. András Jóri
H-1051 Budapest
Nádor utca 22
Hungary
Phone: + 36 1 4757186
Fax: + 36 1 269 3541
E-Mail: adatved@obh.hu

Italy

Garante per la Protezione dei Dati Personali
Segretario generale
Francesco Pizzetti
Piazza di Monte Citorio n. 121
I - 00186 Roma
Phone: + 39 06 69 677.1
Fax: + 39 06 69 677.785
E-Mail: garante@garanteprivacy.it

The Netherlands

College Bescherming Persoonsgegevens
President: Jacob Kohnstamm
Juliana van Stolberglaan 4 - 10
NL 2595 CL Den Haag
Postbus 93374
NL 2509 AJ Den Haag
Phone: + 31-70-88 88 500
Fax: + 31-70-88 88 501
E-Mail: info@cbpweb.nl

Sweden

Datainspektionen
Director General Göran Gräslund
Box 8114 / Flemminggatan 14
S - 104 20 Stockholm
Phone: + 46 8 657 6100
Fax: + 46 8 652 8652
E-Mail: datainspektionen@datainspektionen.se