Joss Wright—Ed. (Oxford Internet Institute, *Ethics Advisor*)
Aggelos Kiayias (University of Edinburgh)
Thomas Zacharias (University of Edinburgh)
George Danezis (University College London)

Ethics Report

Deliverable D1.4

31st October 2016
PANORAMIX Project, # 653497, Horizon 2020
http://www.panoramix-project.eu

Horizon 2020
European Union funding
for Research & Innovation

Revision History

Revision	Date	Author(s)	Description
0.5	2016-07-31	JW (OII)	Initial draft
1.0	2016-08-31	JW (OII)	Final version and submission to the EC
1.5	2016-10-03	TZ (UEDIN)	Requirements tables for each partner
1.7	2016-10-10	GD (UCL)	Detailed procedures for UCL ethics review process.
1.5	2016-10-17	TZ (UEDIN)	Integrated input from partners regarding implementation.
1.8	2016-10-20	JW (OII)	Minor edits
2.0	2016-10-31	AK (UEDIN)	Revised final version and submission to the EC

Executive Summary

Following the grant agreement the ethics report has a three-fold objective.

1. It details all procedures that will be implemented for data collection, storage, protection, retention and destruction and confirmation of personal information by PANORAMIX partners.
2. It provides copies of ethical approvals by the competent Ethics Committee and copies of approvals for the collection of personal data by the competent University Data Protection Officer or National Data Protection authority and any relevant authorisations, if applicable.
3. It contains templates of the informed consent form to be used.

The document is structured in three chapters, reflecting the above objectives.

Contents

1. Introduction

1.1 Purpose of document

This document sets out ethical considerations raised by the PANORAMIX project, and identifies areas in which attention should be focused. Whilst a number of ethical issues in PANORAMIX relate to data protection requirements, this document is not focused on legal compliance with European data protection regulations. This document does not set out a proscriptive guide to research ethics or attempt to enforce an idea of correct ethical behaviour. Instead this document identifies ethical questions raised by the project, with the intention that these questions will be considered by project researchers, rather than to define the answers to those questions.

1.2 Project Goals

PANORAMIX aims to develop a privacy-preserving communications infrastructure based on mix networks that can be exploited by European businesses. The core goal of the project is to develop a practical and scalable underlying mix-net infrastructure that will support a range of possible future applications; in the project itself this infrastructure is to be applied to three specific use-cases. The example applications in the project comprise: mix-nets for electronic voting, privacy-preserving cloud service provision with support for anonymised aggregate surveys and statistical analysis, and privacy-preserving messaging. Each of these example applications is supported by a partner with an existing customer base that provides the initial test-bed for the technology.

In each of these cases the goals of PANORAMIX are to add or improve a privacy layer over services that are already offered by the commercial partners. Due to this, data protection requirements will, in each case, fall under the existing relationship that those partners have with their users unless significant alterations are made to the service or if extra user data are gathered, stored, or processed. There are some key clarifications to this, which will be discussed below, however it is worth noting that for each partner, procedures for storage and processing of personal data are already in place, and the projects use cases are not anticipated to gather any extra data or require further procedures. Existing policies for handling of data are appended to this document.

2. Procedures

2.1 Legal Framework

The European Data Protection Directive [Directive 95/46/EC] sets out a key element of the ethical considerations for a project such as PANORAMIX, in which the major concerns are the storing, handling, and processing of data concerning European citizens. It is worth noting that Directive 95/46/EC is due to be replaced by the recently-adopted General Data Protection Regulation (GDPR) [Regulation (EU) 2016/679] in mid-2018. The modifications in data management regulation that are put in place by the GDPR are reflected in this report so that it is ensured the outcome of the project will be compliant with the new regulation.

2.2 Personal Data

Personal data are defined as: any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;" (Directive 95/46/EC Article 2(a)) Within the context of PANORAMIX, this refers to identifiers such as names, email addresses, and user accounts; messages, stored documents, and other data linked directly to individual users of the services involved in the case studies. Personal data may also be encountered by academic partners in the course of research on live internet trace. This second case will be discussed in greater detail below.

2.3 Data Management

We provide the background principles for all the data management procedures of concern with respect to the PANORAMIX project, namely, data collection, storage, protection, retention, destruction and confirmation.

2.3.1 Data Collection

Data should be collected for specified, explicit and legitimate purposes. The data collection process should allow the data subjects to give their consent. The purpose of data collection should be explicitly determined at the time of the collection. In case of statistical purposes, the result of processing is aggregate data and not personal.

2.3.2 Data Storage

The storage period should be reasonable with respect to the processing purposes. The data should not be stored more than necessary and solely for the purposes for which they were collected. In case of any detected data loss, the data subject should be informed without delay.

2.3.3 Data Protection

The key principles that apply to personal data protection are detailed here

- data processing should be authorised and executed fairly and lawfully. In case of any detected alteration or unauthorised disclosure, the data subject should be informed without delay.
- special categories of processing: it is forbidden to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. This provision comes with certain qualifications concerning, for example, cases where processing is necessary to protect the vital interests of the data subject or for the purposes of preventive medicine and medical diagnosis.
- the data subject should have the right to object, on legitimate grounds, to the processing of data relating to him/her. He/she should also have the right to object, on request and free of charge, to the processing of personal data that the controller anticipates being processed for the purposes of direct marketing. He/she should finally be informed before personal data are disclosed to third parties for the purposes of direct marketing, and be expressly offered the right to object to such disclosures.

2.3.4 Data Retention

The data controller should facilitate the data subject to access, rectify their data and practice his/her 'right to be forgotten' [GDPR, Article 17]. In addition, the controller should not hinder any attempt of the data subject to transfer the collected data to another controller [GDPR, Article 20].

2.3.5 Data Destruction

The data controller should evaluate the risks of accidental or unlawful data destruction. In case of any detected destruction the data subject should be informed without delay.

2.3.6 Data Confirmation

Data processing should be performed transparently with respect to the natural persons concerned. The data controller must provide the data subject from whom data are collected with certain information relating to himself/herself (the identity of the controller, the purposes of the processing, recipients of the data, etc.). The data subject should be able to receive confirmation of their data processing. Easy-to-understand information on processing details should be available to the data subject.

2.4 Implementation - Academic Partners

The academic partners in the project, with the exception of UCL, do not collect personal data for experiments, research or any other purpose within the PANORAMIX consortium. For this reason, this report does not provide any information about the data management implementation procedures carried out by partners UEDIN, UoA, UoT, KUL.

Partner UCL, as part of WP3, designs and evaluates new designs for mix network, especially for messaging (to support WP7), as well as novel techniques for privacy preserving statistics and data collection (to support WP6). As part of these activities, UCL may request some data from other user-facing partners, that is derived from users, and thus personal data, to evaluate designs under realistic and ecologically valid usage loads.

We note that the purpose of some data collection will be the development of privacy-friendly statistics collection and aggregation. Thus, the processing of personal data themselves will be the first to benefit, in terms of privacy, from the PANORAMIX advances. Such procedures were already researched as part of WP3 for the purpose of collecting distributions of data items, such as the aggregate statistics discussed in

> Luca Melis, George Danezis, Emiliano De Cristofaro: *Efficient Private Statistics with Succinct Sketches.* 23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016.

Two key categories of user derived data are foreseen to be of use to the activities of the UCL partner:

1. **Aggregate statistics:** Those relate to the dynamics of the traffic in messaging systems, such as those managed by Mobile Vikings. Those statistics, include the distribution of message sizes, the distribution of the length of conversations, the distribution of latencies of message delivery and responses, and distributions of media or attachment sizes. The purpose of this collection is to evidence and evaluate mix networks and anonymisation procedures as part of the PANORAMIX project and its outputs.

2. **Granular anonymised traffic records:** For the purpose of testing the performance of designed mix systems, as well as anonymisation procedures, granular anonymised traffic records may be requested from user-facing partners to act as (i) test and evaluation inputs to the private statistics procedures, and (ii) loads for the evaluation of mix systems. The granular records will be anonymised by removing identifiers and replacing them with tokens unlinkable to the accounts concerned. However, unlike the aggregate statistics above for which we can guarantee with high assurance a good degree of unlinkability to raw data records, those granular records may be used alongside side information to de-anonymise them. Since we treat anonymised granular records as personal information, the full UCL Ethics approval process will have to be invoked for UCL to process such data. More information about this process is provided in Section 3.1.

The implementation procedures for academic partner UCL for the two key categories are presented in the following tables:

Procedure	Academic Partner UCL - Aggregate statistics:
Collection	The aggregate statistics are based on raw existing business records collected by user-facing partners (such as Mobile Vikings). Those raw records are aggregated at the point of collection to produce distributions, and provided as such to UCL. The aggregation will be appropriate to ensure no information any single individual is linkable back to that individual thus rendering them anonymised statistics at the point UCL collects them.
Storage	Given the low-sensitivity in terms of the Data Protection Act of anonymised aggregate statistics the datasets will be stored on researchers' main computers, and protected in-line with other business confidential data.
Protection	Anonymisation is applied at the point of collection as the key protection mechanism. Concepts and mechanisms implementing differential privacy properties will be used to ensure no individual information leaks from the dataset.
Retention	The data has to be retained until the publication of all scientific articles output from the project, possibly up to 12 months after the end of the PANORAMIX project, to ensure any requested revisions to the works can be carried out. Subject to a discussion related to the quality of protection and the strength of differential privacy, some of the aggregated anonymised data may be made available to the scientific community for the purposes of scientific reproducibility.
Destruction	In case aggregates are not needed after the above retention period, and those that are deemed either still sensitive or not needed for further scientific inquiry, the data will be deleted using the safe delete option offered by commodity operating systems.
Confirmation	Since the data are anonymised and aggregated users cannot be individually notified of the deletion, but the partners will be notified of the deletion and consulted before any sharing (even for aggregated and anonymised data, that may still be business sensitive).

Procedure	Academic Partner UCL - Granular anonymised traffic records:
Collection	The collected data concerns business and traffic records that are already being collected from user-facing partners for the purpose of managing and improving their services. The purpose of this collection is compatible with the aims of PANORAMIX WP3 and WP6 / WP7 for which we propose to collect the data. This will have to be confimed by the legal department of partners, once the exact nature of data needed is clear (Year 2 and Year 3), and the UCL Ethics committee.
Storage	The data will be stored on an encrypted external hard disk that is maintained in locked facilities at UCL. Access to the hard disk (physical) and cryptographic keys (logical) will be controlled by the UCL PI and only given to staff directly working on WP3 and WP7.
Protection	The granular traffic records will be protected, at the point of collection, by replacing all identifiers with tokens to ensure that incidental re-identification is not easy. However, we note that such a protection protects against UCL researchers that do not have access to side-information, but may not protect anonymity sufficiently against others that have access to enough side information to de-anonymise the records. For this reason we will impose a security policy that forbids the sharing of the granular data.
Retention	The granular data will be retained until all publications relating to PANORAMIX have gone through peer review, to ensure repeatability of experiments and results, and changes requested by the scientific community can be implemented. We foresee that this will be no longer than 12 months after the conclusion of the project.
Destruction	Once the retention period has passed the logical hard disk key will be deleted making the data unusable. The hard disk will be deleted using the secure deletion facility of commodity operating systems.
Confirmation	Since the granular records are anonymised, it is not possible to notify end-users users of the deletion of specific records. However, UCL will notify the partners from which the data was collected that the data was deleted. Under no circumstances UCL will share the data with other parties.

2.5 Implementation - Industry Partners

The industry partners of the consortium that handle personal data are connected with the three use-cases, which are associated with an industry partner, as shown in the table below.[1]

Case Study	Consortium Partner
Private Electronic Voting Protocols	GRNET
Privacy-Aware Cloud Data Handling	SAP
Privacy-Preserving Messaging	Mobile Vikings, Greenhost

In each case, the partner has a pre-established relation with its customers and is engaged with PANORAMIX with the only objective to improve the privacy protection of the existing services that are provided to its customers. This will not result to any fundamentally new provision for

[1]The industry partner Mobile Vikings has been removed from the consortium on September 27th, 2016, however, the ethics report was performed based on information collected in Year-1 of the project.

their users, and as such the underlying data protection agreements are not affected by the new service. Thus, in the below sections we report on the existing data management procedures that are used stressing that these procedures were not put in place for the purpose of PANORAMIX.

2.5.1 Private Electronic Voting Protocols (GRNET)

GRNET operates the Zeus electronic voting platform, which has been in use for over two years. This platform already provides privacy-preserving electronic voting through a specific mix-net implementation. The goals of PANORAMIX are to scale and improve the privacy protections of this platform.

The Zeus platform administers the generation and distribution of voters' credentials, vote collection, and posting of the tallying authorities' public data and all other information required for monitoring the election. The implementation procedures are presented in the following table:

Procedure	**Private Electronic Voting Protocols (GRNET)**
Collection	The electoral committee is responsible for entering the voter registration data (that is, the electoral register). This contains name, surname, father/mothers name, e-mail, phone number. It may also contain an eduGain principal ID. The electoral committee asks the users consent to vote electronically, informing them that their registration data will be stored in an electronic electoral register. The web server hosting Zeus (Apache) keeps a log of accesses and IP addresses. The information on which voters have voted is available to the electoral committee through the Zeus interface, and is consistent with the standard practice in paper ballots, where voter names are stricken off the electoral roll. The web server logs can provide only the access patterns and cannot violate anonymity as everything is encrypted with the election keys. The access patterns may reveal the location of the user when voting.
Storage	The voter registration data are stored in unencrypted form only to be used for future elections.
Protection	The data are protected according to the procedures set by GRNET's Networks Operations Centre; this does not offer any extra protection to voting data, but the voting data that is stored consists only of web server logs, as explained above, and anonymised (through mixnets) ballots and proofs. This information is also downloadable by the electoral committee and could be be published without any inherent privacy risk.
Retention	The users of the system (voters and electoral committee) can access their data (ballots, voter voting data) and download them. GRNET does not have a formal retention or erasure policy yet as such is still subject to regulation for e-voting in Greece; in fact, the to date experience shows that electoral committees request that GRNET will retain voting data, even though no such commitment has been made. As voting data accumulates with the increasing number of elections, a formal GRNET retention policy will be adopted and will be in compliance with e-voting regulation (when legislated).
Destruction	The data are protected by unlawful destruction in the same way that all data in GRNET services are. As explained above, voting data are not treated separately.
Confirmation	The user is informed of every election procedure that his/her data are processed. This is supported via the user's personal mail and verification of the public election transcript.

2.5.2 Privacy-Aware Cloud Data Handling (SAP)

SAP currently offers an encrypted database solution called SEEED. PANORAMIX research will improve the ability of SAP to extract key performance indicators (KPIs) from this existing encrypted service. The key performance indicators will be gathered at an aggregate statistical level, with strict privacy guarantees.

Data (survey answers) are collected and provided as input to standard big data type of aggregate analysis. In surveys, customers are often asked to provide sensitive data (e.g. health, religion, business secrets, etc.) which need to be strongly protected. This is currently carried out according to SAPs existing Global Data Protection and Privacy Policy, reproduced in Appendix A.2 of this document. The procedures' implementation under the agreement's conditions are summarised in the following table.

Procedure	Privacy-Aware Cloud Data Handling (SAP)
Collection	Data are collected only after the customer's consent and only for fulfilling the specified processing purposes.
Storage	Personal data are stored only for as long as is absolutely necessary for the purposes specified or other legal requirements. Thereafter, personal data are deleted or anonymised. Inaccurate data are corrected or deleted as soon as possible.
Protection	There is continuous monitoring that data processing is in line with applicable law. Every employee and every third party acting on behalf of SAP are instructed that they are not permitted to process personal data without authorisation. If personal data is to be exchanged within the SAP Group or with other companies, it must first be checked whether contractual agreements on data protection and privacy and data security are required.
Retention	Continuous legal monitoring is applied to ensure compliance with any data retention requirements that arise in a case-by-case basis.
Destruction	Continuous legal monitoring is applied to ensure compliance with any data destruction requirements that arise in a case-by-case basis.
Confirmation	Following the terms of agreement, a person affected may, at any time, request information about the data stored on them, its origin, purpose for storing, and recipients to whom the data is passed on.

2.5.3 Private-Preserving Messaging (Greenhost, Mobile Vikings)

Greenhost

Currently, for the purposes of PANORAMIX data collection has only been performed on anonymized metadata, with no personally identifying information. The data collection was email metadata over a four hour time period that was provided to UCL in order to help parameterise and design the PANORAMIX mix network. See Deliverable 7.1 for instructions on how the data was collected in aggregate and anonymised. In PANORAMIX, Greenhost will continue work with the PrivEx-based approach of UCL keeps data provably anonymized and not maintain entire databases, but only "succinct sketches" of databases[2] that cannot be de-anonymized but maintain the crucial information needed for PANORAMIX such as average delivery time and average number of messages per epoch.

We will inform users via a PANORAMIX-specific special agreement if individual outbound or inbound email is logged. In this case, the customer will be bound by Article 6 "Experimental

[2]Luca Melis, George Danezis, Emiliano De Cristofaro: *Efficient Private Statistics, with Succinct Sketches.* NDSS 2016.

Software" of the terms of agreement. More information about Greenhost procedures are shown in the table below.

Procedure	Private-Preserving Messaging (Greenhost)
Collection	Data collection is never performed on an individual, but Greenhost does use statistics on data in order to both identify what services are working and how they are performing. This is captured in article 5.4 of Greenhost's customer agreement, which is explicitly agreed with by every customer of Greenhost.
Storage	Data collected for measuring the performance of PANORAMIX is kept for 30 days. The data is then sent to UCL for analysis, but locally the data are then deleted. An archival copy may be captured by regular back-ups of the Greenhost system, but archives are only kept in general for 6 months. Thus, there is no long-term storage of even anonymised data for PANORAMIX analysis by Greenhost.
Protection	Article 10 states that data will not be gathered without consent and Greenhost is governed by Dutch law which includes the Dutch data protection act. In detail, in Article 10.2 "Greenhost will not take cognizance of data stored by the customer...unless with the Customer's consent, access has been necessary for performance of the contract or Greenhost is required to do so under a statutory provision or authorized order by the authorities. In that case Greenhost will endeavour cognizance of the data to minimize, to the extent with its power and, if possible, inform the customer of this application in an up to date manner."
Retention	Greenhost follows the current Data Protection Regulation, and will continue to follow the GDPR. This gives customers the ability to demand deletion or modification of their data. Greenhost will comply with all Dutch data retention laws. However, currently although it has been debated in the Dutch parliament, there is currently not a Dutch Data Retention directive and so data retention is covered, as noted earlier, by Article 5 of the customer agreement and so data is only retained to optimise services. In general, Greenhost does not retain individual traffic or even IP addresses of its customers.
Destruction	The data destruction policy is covered in Article 10 of the agreement. Note that this right continues after the customer has left Greenhost, as Article 10 states that "The obligation of this article will remain after the termination of the Agreement for any reason, and so much for so long as the providing party can reasonably claim to the confidentiality of the information. Although this is not explicit, "Unlawful destruction" would be a violation of the Contract by Greenhost, as the service contract requires the data be available to the customer by the definition of the Service.
Confirmation	Greenhost logs data automatically when needed in terms of performance, but only in aggregate without individual logs (See Deliverable 7.1 for details). Therefore, Greenhost does not ask the individual customer to confirm if the data is original or correct. However, if a sample of data is collected for performance, any deviations would be detected from other samples and could lead to an investigation. Also, in terms of PANORAMIX, the aggregate anonymized data are also being analyzed by UCL, who should detect anomalies and help confirm our analysis of how email traffic can work with a PANORAMIX-enabled mix net.

Mobile Vikings

Mobile Vikings offer mobile phone services to users, with the option to sign up to an active Viking Lab that allows participation in developing mobile technologies and services. This existing user base, who make an explicit choice to engage in individual experimental services, will be the target of the developed PANORAMIX messaging application.

The customers of Mobile Vikings are granting the management of their personal data under the Privacy Conditions Agreement reproduced in Appendix A.4 of this document. The procedures implementation under the agreement's conditions are summarised in the following table.

Procedure	Private-Preserving Messaging (Mobile Vikings)
Collection	Mobile Vikings keep record registration data that contain: first name, last name, address, email address, date of birth, phone number. Information is requested from the customers when they send emails to verify registration data. In case of customer contacting, Mobile Vikings may link the contact to the customer's registration file, if necessary.
Storage	The registration data and the data regarding the customer's transaction with Mobile Vikings are included in a permanent record.
Protection	Among a list of legitimate use purposes, customers consent that their data are processed for handling their orders and bills, conducting market research, Mobile Vikings management, resolution of legal disputes, etc. On simple request, the customers can oppose the use of their private information for purposes of direct marketing.
Retention	On simple request, the customers can access, correct, rectify and/or change their data.
Destruction	The company is compliant with all regulations of Belgian law according to data destruction.
Confirmation	The customers are able to verify the validity of their personal record on simple request.

2.6 Notes on Data Procedures

In this section, we provide comments on data processing issues directly related to the project goals that could be given longer-term consideration.

2.6.1 Loss of Personal Data

Traditional messaging and storage services operate on the basis of trust in the provider to maintain adequate protection for data whilst retaining the ability to access that data if required. Encrypted storage and messaging removes both the requirement for trust in the operator, as well as the ability of the operator to retrieve data on behalf of a user whose credentials have been lost. Fundamentally, little can be done here beyond informing users of the inability of the operator to retrieve private data. With increasing usage and awareness of encrypted storage, such as full disk encryption for platforms such as Microsoft Window, Apple Mac OS, Android, and iPhone iOS, users are increasingly aware of the inability of providers to retrieve correctly encrypted data on demand.

2.6.2 Data Retention

Following the April 2014 decision of the Court of Justice of the European Union in a case brought by Digital Rights Ireland (C-293/12), the EU Data Retention Directive (Directive 2006/24/EC)

was ruled unconstitutional on the grounds that bulk collection of personal data failed to be necessary and proportionate for the purposes of law enforcement. In light of this decision, prior existing requirements for communication providers to store data regarding customer telecommunications are no longer in force at the European level, although the specific status of national laws that transposed the Data Retention Directive is in some cases contested. As such, any interaction that data retention requirements might have previously had with respect to the services offered by PANORAMIX are no longer relevant.

2.7 Summary

This completes the description of data management procedures as implemented by the PANORAMIX consortium partners. The academic partners, with the exception of UCL, do not engage in data collection within the consortium and thus no information is provided regarding their procedures. For the remaining partners, only UCL has specific procedures put in place for the purposes of the PANORAMIX project. The industry partners, GRNET, SAP, Greenhost, and Mobile Vikings, engage in the consortium under their pre-existing relationships in terms of data management with their user base.

It is important to stress that the PANORAMIX system does not change the nature of existing data management procedures (collection, storage, protection, retention, destruction and confirmation) for these partners and neither poses a hindrance in terms of the ability to comply with current and future regulations in data management. In fact, the employment of the PANORAMIX system will be an argument assisting in compliance arguments, since it enables data management procedures related to collection, storage and protection to enjoy an improved anonymity profile in comparison to a non-PANORAMIX enhanced deployment.

3. Approvals

3.1 Academic partners (UCL)

The only academic partner engaging in data collection for research is UCL. All research proposals involving living human participants and the collection and/or study of data derived from living human participants undertaken by UCL staff or students on the UCL premises and/or by UCL staff or students elsewhere requires ethical approval to ensure that the research conforms with general ethical principles and standards.

As documented on the UCL website relating to research Ethics, ethical approval at UCL follows a 10 step process, dependant on the nature of the research undertaken. However, blanket pre-approval is not possible (say for all potential activities in PANORAMIX), and individual approvals will be necessary depending on the specifics of the data and research conducted. For this reason, there is no copies of approval that can be supplied at this stage. Nevertheless, these will be sought and acquired in year-2 and year-3 of the project as needed and following the procedure outlined below.

- **Step 1:** Researchers are advised to submit approvals being mindful of the deadlines and timelines necessary for the Ethics committee to consider the application. The committee meets about once a month.

- **Step 2:** Researchers register within the Ethics database [5], with personal details, if not already registered. If this is a first application to the Committee, a personal account will be established. Otherwise, the proposal will be added to the researcher's account which can be viewed when they enter the site http://ethics.grad.ucl.ac.uk/new_user.php

A unique Project ID for the proposal will be issued. The finance department will require this Project ID in order to process grant applications based on this research. Once a Project ID has been issued, the application form and guidelines will be available for download. A sample copy of the documentation can be viewed below.

- **Step 3:** (not required for PANORAMIX research) Formal Sponsorship Review for Clinical Trials Conducted in Developing Countries.

- **Step 4:** (not required for PANORAMIX research) Disclosure and Barring Service (DBS) Checks. A criminal record check will be required by law if the research includes working in 'Regulated' activity with vulnerable groups as defined by the Safeguarding Vulnerable Groups Act 2006 or in a position of trust as defined by the Rehabilitation of Offenders Act Exception Order 1975. Please note that UCL, in accordance with DBS guidelines, does not accept portability of DBS checks which UCL staff or students may have from previous organisations as proof of satisfactory clearance.

- **Step 5:** (required for PANORAMIX) Data Protection. The subject can register for Data Protection on the website by downloading 'Form 2: Research Registration Form' [6]. The form should be completed on-line and e-mailed to: data-protection@ucl.ac.uk. The Legal Services should be able to process your application within 5 days upon which time you will be issued with a Data Protection Registration Number[1]. Please quote your data protection registration

[1] See https://www.ucl.ac.uk/finance/legal/dp-foi-overview

number in section A2 of the application form as evidence that the project has been registered with the UCL Data Protection Officer.

- **Step 6:** Risk Assessment. In order to determine whether there are any risks associated with your research i.e., risks to yourself as the researcher and to those you are researching, it is important to carry out a risk assessment. It is a legal requirement that all research is assessed for risk. Submitters can refer to UCL Safety Services guidance on how to carry out a risk assessment. The guidance includes how to record the assessment which must be authorised by your Supervisor and retained for the submitters' records.

- **Step 7:** (not required for PANORAMIX): Insurance. The insurance for all UCL studies is provided by a commercial insurer. For the majority of studies the cover is automatic. However, for a minority of clinical research studies the insurer requires prior notification of the project before cover can be provided. Travel Insurance arrangements for students conducting research overseas — for studies conducted overseas an application form will need to be completed so that an insurance cover note can be issued.

- **Step 8:** Completion of the application form and appendices that are applicable to the study ensuring that both the Principal Researcher and the Head of Department have signed the form. The Head of Department should also indicate on the form whether the application is being submitted for (a) Chair's action or (b) Full Committee Review based on the criteria of minimal risk.

→ Application Form: http://ethics.grad.ucl.ac.uk/forms/appform_sample.pdf

→ Application Guidelines: http://ethics.grad.ucl.ac.uk/forms/guidelines.pdf

→ Model Participant Information Sheet and Guidance: http://ethics.grad.ucl.ac.uk/forms/model-participant-information-sheet-and-guidance.pdf

Recruitment Documents for Participants. All studies that involve the recruitment of participants will use recruitment documents such as information sheets and consent forms. For example forms as well as guidance on formulating your participant information sheet (see Advice on Formulating Participant Information Sheets http://ethics.grad.ucl.ac.uk/advice.php).

- **Step 9:** When the application is complete, submitters are strongly encouraged to mail physical copies of their application and supporting documentation, either via the internal UCL mail or externally to the following new address, rather than in person, as access will be an issue at 1-19 Torrington Place. If the application is for full committee review 13 double-sided copies will be required and for Chair's review, 2 copies.

INTERNAL Mailing Address	EXTERNAL Mailing Address
Helen Dougal	Helen Dougal
Research Ethics Co-ordinator	Research Ethics Co-ordinator
Academic Services	Academic Services
1-19 Torrington Place (9th Floor)	UCL
UCL	Gower Street
	London
	WC1E 6BT

An electronic copy should be also submitted to ethics@ucl.ac.uk

- **Step 10:** Following Approval. The Principal Researcher must report any proposed changes, any adverse events and if required report progress on an annual basis (see Key Responsibilities of the Principal Researcher following Approval http://ethics.grad.ucl.ac.uk/responsibilities.php).

3.2 Industry partners (GRNET, SAP, Greenhost, Mobile Vikings)

As it will explained already in Section 2.7 (see also Section 4.2), for all of PANORAMIX users engaged in the main case studies run by the Consortium industry partners, personal data are processed in a fully consistent manner with respect to related partner's Terms and Conditions that the users have already consented. Therefore, further approval documents for data processing by industry partners are not applicable.

4. Informed Consent

Informed consent is a key principle of ethical research, ensuring that research participants are adequately informed of the risks of taking part in experimental studies, that their participation is voluntary, and that the information about them gathered remains under their control. The two key principles of informed consent, taken here from the ESRC Framework for Research Ethics (http://www.ethicsguidebook.ac.uk/consent-72), can be defined as:

- **Principle 1:** Research subjects must be informed fully about the purpose, methods and intended possible uses of the research, what their participation in the research entails and what risks, if any, are involved.
- **Principle 2:** Research participants must participate in a voluntary way, free from any coercion.

We analyse how PANORAMIX project data processing activities comply with the two key principles separately for the involved academic and industry partners.

4.1 Academic partners (UCL)

As mentioned in Section 2.5, the academic partners in the project, with the exception of UCL, do not collect personal data for experiments, research or any other purpose.

Regarding partner UCL, all experiments that may result in data capturing due to measurement of internet traces, will be performed only after the approval of UCL's Ethical Committee (see Section 3.1), whose standards not only respect informed consent (hence Principles 1 and 2) but also the participants' right to confidentiality and the balancing of their involvement against the potential benefit of the conducted research to the overall community.

The UCL partner does not collect data directly from users, but only indirectly though the user-facing partners of the project. We foresee such collection is lawful under the existing Privacy Statements of the partners (such as Mobile Vikings) allowing the collection of information for the purposes of monitoring and improving their services.

All the data collected is anonymised, at the point UCL receives it – in a very strong sense when it comes to aggregate data, and in a sufficient manner with respect to data protection when it comes to granular records – thus making the legality of the collection a matter for the user-facing partner and placing UCL in a role of Personal Data Processor rather than Personal Data Controller. Thus UCL will have to abide by the privacy statement of the partners.

In extremis, in case specific and identifiable data needs to be collected, UCL will advise the user-facing partners about the form user notice and consent needs to take. UCL has clear guidelines on how to formulate such consent forms as documented in http://ethics.grad.ucl.ac.uk/forms/model-participant-information-sheet-and-guidance.pdf and http://ethics.grad.ucl.ac.uk/advice.php

In all cases, and in the spirit of the UCL Ethics approval which requires strong data minimization and purpose limitation, such consent forms can only be drafted once the exact nature of

the collection and processing purpose is known in Year 2 and Year 3. However, all institutional procedures and processes are in place once this is necessary.

4.2 Industry partners (GRNET, SAP, Greenhost, Mobile Vikings)

All subjects that engage as customers in the standard activities of the partners GRNET, SAP, Greenhost and Mobile Vikings consent to their data processing according to the terms and conditions agreement of each partner, provided in Appendices A.1, A.2, A.3 and A.4 respectively. As presented in Subsections 2.5.1 2.5.2 and 2.5.3 all three agreements are consistent with EU data protection and privacy regulations, therefore preserve Principles 1 and 2. PANORAMIX project activities related to industry partners comply with the said principles by being fully consistent with the terms and conditions of each partner's agreements. In particular,

- GRNET's existing data protection and usage agreement, "Terms and Conditions", are specified with respect to the existing electronic platform. Applying PANORAMIX mix-net into the Zeus e-voting system and combined with the privacy protections already in place that anonymise personal data with respect to the use of the service, GRNETs existing data protection and usage agreements do not need alteration for the purposes of PANORAMIX.

- In surveys, SAP customers are often asked to provide sensitive data (e.g. health, religion, business secrets, etc.) which need to be strongly protected. Beyond existing customer data covered by SAPs existing Global Data Protection and Privacy Policy, no personal information processing will be carried out for the purposes of PANORAMIX.

- The customers of Greenhost are providing data based on the existing "Usage Terms and Conditions." The type of data collection for PANORAMIX purposes is consented as part of "Article 6. Experimental Software" in the agreement and are used solely for the optimisation of the operation of the messaging system.

- The customers of Mobile Vikings are granting the management of their personal data under the Privacy Conditions Agreement. The user base for the PANORAMIX Private-Preserving Messaging use case consists only of already existing customers of Mobile Vikings. Consequently, the customers' relationship with Mobile Vikings as a data controller, in combination with their explicit consent to make use of the service, do not require alteration to existing agreements.

4.3 Summary

As far as academic partners are concerned, only partner UCL's foreseen engagement may result in data processing and this will be done under the restrictions of UCL Ethical Committee's approval, see Sections 3.2, and 4.1.

Apart from the UCL partner's upcoming activities, the research in PANORAMIX, and certainly in the main case studies developed by industry partners, does not involve the gathering of personal data in the form envisioned by traditional informed consent scenarios in research. In these case studies, direct user experimentation is limited to the extension and improvement of privacy protections in systems with which users are already familiar, and for which users have made an active decision to take part.

> **Ethics Advisor Statement.** Users in PANORAMIX are not directly studied, subjected to treatment, asked to complete tasks, surveyed, or analysed individually. As such, as ethics advisor I am of the opinion that seeking additional informed

consent for participation in the main case study research is unnecessary unless the specific details of the research are later determined to place users at extra risk with respect to the exposure of their personal data.

5. Conclusions

The PANORAMIX project is chiefly concerned with adding enhanced privacy considerations to existing services. In each of the use cases electronic voting, cloud platforms, and mobile messaging the experimental privacy enhancements do not entail a new service or experiment in which new forms of personally-identifying information are gathered, but instead make use of existing services. As such, the existing data protection agreements and procedures for those services do not require amendment.

Academic work at partner UCL may utilise data collected by partner Greenhost to improve the efficiency and fine tune the messaging application. Researchers at UCL will engage with their institutional research ethics committees, and will practice data minimisation and anonymisation techniques to remove or delete immediately all data beyond that required to test their techniques. The procedures to be followed have been thoroughly documented in this report.

> **Ethics Advisor Statement.** As ethics advisor to the project, I am satisfied that the research in the project has been designed with full consideration for ethical concerns, and that the appropriate measures are in place for compliance with data protection and informed consent of users to participate in the research. The PANORAMIX project is unusual, in some senses, in that the goals of the project intrinsically aim to improve many of the traditionally-considered ethical concerns related to data privacy and security. Further, the research of the project relies on modifications to existing services that improve, rather than compromise, the protections of users. Despite this, the nature of the project does raise some broader ethical considerations beyond the basic compliance with data protection. These considerations, relating to the provision of strongly-anonymous services, with the accompanying potential for untraceable abuse and criminal activity, have been raised and actively discussed at project meetings. While such questions do not admit to easy answers, as ethical advisor I am satisfied that consideration of these questions have been fundamentally incorporated into the research of the project and in fact an upcoming deliverable (D1.5, "System Abuse / Misuse and Mitigation Strategies") will address them.

A. Data Usage Agreements

This section reproduces the applicable data usage agreements, terms of service, or privacy policies in place for the commercial project partners.

A.1 GRNET Terms and Conditions

GRNET Terms and Conditions (Legal Report)

General

GRNET S.A. has privacy policy documents for particular services it offers. The details and specifics of the privacy policy of each service are defined accordingly, in close cooperation with the Hellenic Data Protection Authority (HDPA), depending on the nature and the requirements of each service.

An example of such a Privacy Policy document, that applies to GRNET S.A. IaaS Service ~okeanos (http://okeanos.grnet.gr), and is part of its Terms Of Use is as follows:

"In order for GRNET SA to provide its services without any impediments, GRNET S.A. can collect general statistical data regarding the flow and optimization / development of the network and computer resources of the infrastructure. GRNET S.A. does not have direct access, has no interest in and will not collect any specific data with regard to specific services which are hosted in virtual machines or by the final users of the hosted services. The information which will eventually be collected through the services by GRNET S.A. will be used according to the institutional framework in force in Greece and in the European Union.

This data can be used in order to monitor the function of the services, to improve the quality of its function, or for research purposes, and can be published or distributed to third parties after a prior appropriate elaboration so that personal data of the managers and / or of the final users are not disclosed. GRNET S.A. can disclose information regarding the use of virtual machines when it is demanded by the law and the competent services."

The Zeus e-voting system

In the PANORAMIX project GRNET will work on its Zeus e-voting system (http://zeus.grnet.gr). The Zeus system is used by both election committees, who administer elections, and voters, who cast their votes. The users are currently not asked to accept a privacy policy. From a user-experience point of view this is a complicated issue, as voters interact with a system only in the context of an election. Asking voters to accept a document in order to vote entails the possibility of voters not voting by not accepting. At the same time, not informing voters at all about terms of use is far from ideal; GRNET S.A. will work on that in the course of the project.

Zeus Information Collecting

Voters are listed with their contact details so that Zeus can send them an invitation to cast their ballot. These details, e-mail and/or phone numbers are provided by election authorities and Zeus stores them indefinetely as part of the election authorities account with the system, but does not use it in any other way.

Zeus logs every action of authenticated voters, trustees, and election administrators for audit purposes. This information is used when election authorities order audits or investigations as a response to incidents or claims and challenges from voters and candidates.

By the design of the cryptographic process and the election protocol, Zeus acts as an automatic trustee for all elections thus preventing any manipulation from election authorities.

Cookies

Zeus uses cookies only for establishing a temporary session with the user and does not ask to store cookies for long term.

A.2 SAP Terms and Conditions

SAP Global Data Protection and Privacy Policy

Version 2.0
December 2015

Public

Contents

This page is intentionally empty in the PUBLIC version of the Policy.
Additionally the annexes with internal content are not provided.

1. Introduction

SAP is bound by data protection and privacy laws. SAP respects and protects the rights of individuals, in particular the right to data protection and privacy during the processing and use of information as well as the right to privacy. The protection of information comprises the personal data of employees, applicants, customers, suppliers, partners, and all other persons within SAP's area of responsibility. To adhere to this obligation, SAP has adopted an SAP Global Data Protection and Privacy Policy ("Policy"), and reviews it regularly.

The Policy outlines a group-wide minimum standard for handling personal data in compliance with data protection and privacy laws. It defines requirements for all operational processes that affect personal data, as well as clear responsibilities and organizational structures. As soon as a process at SAP involves collecting, processing, or using personal data, the provisions of this Policy are to be adhered to. Management of the individual SAP group companies and the relevant process owners are responsible for ensuring that all processes during which personal data is collected, processed, or used, are designed such that the provisions of this Policy are fulfilled. It is the duty of all SAP employees to comply with the provisions of this Policy when handling personal data in their daily work for SAP.

SAP is a global company with headquarters in Germany, a member state of the European Union (EU). Therefore, the basic principles established through this Policy are based on the requirements of European data protection and privacy legislation. If, on a case-by-case basis, applicable local law outlines stricter data protection and privacy requirements than this Policy, personal data must be handled in compliance with those stricter laws. Additional standards and/or guidelines within the SAP Group that are issued as a result of this Policy must also take the applicable law into account in this respect. Questions on applicable law can be directed to the Data Protection and Privacy Office ("DPPO") (mail:privacy@sap.com) and/or the appointed Data Protection and Privacy Coordinators ("DPPC").

Data protection and privacy rights of employees must be guaranteed in accordance with the law of the country in which the employment contract with the respective SAP Group company was concluded, notwithstanding the local law of the country in which the employee data is actually processed or used. The legal responsibility for collecting, processing, and/or using the personal data of SAP employees always lies with the respective employer. It is the employer's duty to inform other SAP Group companies (for example, if the manager is an employee of a different SAP company), if within the scope of processing and using personal data for their employees, different provisions apply for the protection of personal data from those defined in this Policy.

This Policy shall not restrict SAP's right to use employee personal data to the fullest extent legally possible in order to preserve its position during any legal action or official proceedings. However, the applicable data protection and privacy law must be observed by SAP generally.

2. Definitions

Anonymized data Anonymous data	Anonymized data is data in a form that makes the direct or indirect identification of an individual person impossible, even with the aid of other data or information. Anonymous data does not have any reference to a person when it is collected. Anonymous and anonymized data is no longer subject to the internal or external data protection and privacy regulations.
Commissioned data processor	A natural or legal person, authority, institution, or any other office that processes personal data on behalf of the data controller, for example, an external company or an SAP company that is not the data controller itself.
Special categories of personal data	Contain data on the racial or ethnic origin, political views, religious or philosophical beliefs, union membership, felonies, penal convictions, health, or sexual preferences of persons, as well as data that can be misused for identity theft, for example, social security numbers, credit card and bank account numbers, as well as passport or driver's license numbers.
Person affected	An identified or identifiable natural person whose personal data is affected by a data processing action. A person is deemed identifiable if he or she can be identified directly

	or indirectly, in particular by reference to an identity number or to one or more factors specific to that person's physical, physiological, psychological, economic, cultural, or social identity.
Data processing actions (collecting, processing, and/or using)	Collecting means procuring data on the person affected. Processing describes any operation performed with or without the aid of an automatic procedure, or any set of operations connected with personal data, for example, collecting, saving, modifying, storing, changing, transferring, locking, or deleting personal data. Using means any usage of personal data except for processing.
Third-party	A natural or legal person, authority, institution, or any other office, except for the following: • The person affected • The office responsible • The commissioned data processor • The persons who, under the direct responsibility of the data controller or the commissioned data processor, are authorized to process the data For the purposes of this Policy as well as applicable data protection and privacy laws, different companies within the SAP Group are classified as third-parties in relation to each other.
Consent	This may be explicit or implicit. Explicit consent generally requires an action by the person affected, through which they allow the processing of data, for example, the declaration of consent with the sending of e-mails, or entering of personal data (opt-in). Explicit consent granted without duress is deemed to be the legal basis for the processing of personal data, provided no other legal provision is in force. Implicit consent (for example, via opt-out) allows processing provided the person affected does not object.
Deletion	Either the physical destruction of data or the anonymization of data in such a way that makes it impossible to relate the data to a natural person.
Personal data	All information on an identified or identifiable natural person (person affected). A person is deemed identifiable if he or she can be directly or indirectly identified, in particular by reference to an identity number or to one or more factors specific to that person's physical, physiological, psychological, economic, cultural, or social identity. For example, persons can be identified directly on the basis of names, telephone numbers, e-mail addresses, postal addresses, user IDs, tax numbers, or social security numbers, or indirectly on the basis of a combination of any information. Personal data that is subject to this Policy includes data on employees, applicants, former employees, customers, interested parties, suppliers, partners, users of SAP websites and services, and any other persons. The data may be contained in an SAP system, or in systems of third parties, who operate these on behalf of SAP. Customer systems that SAP or third parties on behalf of SAP operate are also relevant, as are systems operated by customers themselves if SAP employees can access the personal data stored in these systems while providing services, support, or consulting services.
SAP	SAP SE and its global offices and subsidiaries (and 'affiliates' as defined by the German Stock Corporation Act (AktG), article 15 ff).
Data controller (controller)	A natural or legal person, authority, institution, or any other office that, either alone or in collaboration with others, makes decisions on the purposes and means of processing personal data (general legal definition). In the case of SAP, an SAP company is always the controller for the personal data of its employees, customers, suppliers, partners, or other persons. SAP employees, internal units, or organizations cannot be controllers. The controller is represented by the management legally responsible, for example, by the members of the SAP SE Executive Board, or the directors of other SAP companies.

3. Basic Principles of Protecting Personal Data

During every process that includes collecting, processing, or using personal data, personal data may be processed or used only in accordance with this Policy and to the extent permitted by law.

Processing is only allowed in the following cases:

- If a person affected freely gave their consent, for example, when registering on a website
- If required to fulfill contracts with the person affected, for example, for an employment contract or a service contract
- If legally required or permitted, for example, due to tax or social security laws.

Personal data may be collected and processed for lawful purposes only. The respective purpose must be defined before the time at which the data is collected. Processing for a purpose other than the one defined before the data was collected is permitted in exceptional circumstances only if the person affected consents to the processing or if stipulated by law.

Personal data is to be collected directly from the person affected. Otherwise, the person affected must be at least informed of which types of personal data will be collected, processed, and/or used, and for which specific purposes.

Data may only ever be collected to the extent absolutely necessary for fulfilling the purpose specified before it is processed or used; any other processing is not permitted.

Personal data must be accurate at all times and corrected where necessary.

Personal data may be retained only for as long as is absolutely necessary for the purposes specified or other legal requirements. Thereafter, personal data must be deleted or anonymized (for more information, see section 5b).

4. Responsibilities for Data Protection and Privacy

a. Management

The legal responsibility for collecting, processing, and using personal data within SAP lies with the executives of the SAP company that collects, processes, or uses the personal data for their business purposes.

Within SAP, responsibility can be delegated along the organizational structure of SAP by means of documented instructions from management, guidelines, and business processes that involve the explicit transfer of responsibility to managers at different levels as well as employees.

Management is responsible for structuring all processes during which personal data is collected, processed, or used in such a way that the requirements of this Policy are fulfilled.

The following tasks are the responsibility of management in every SAP company:

- Continuous monitoring of the applicable law
- Ensuring that processes during which personal data is collected, processed, and/or used are in line with applicable law, and that local and global process owners are informed of necessary changes
- Ensuring that all approvals required by the supervisory authorities for collecting, processing, using, and transferring personal data have been granted, and that the necessary notifications have been sent to the supervisory authorities

b. Global Human Resources

Before commencing an activity during which access to personal data cannot be excluded, every employee and every third party acting on behalf of SAP are to be instructed that they are not permitted to collect, process, or use personal data without authorization (data protection) and that this data must be handled confidentially (confidentiality). Employees are to be made aware of the consequences of violating data protection and confidentiality. This Policy

and other internal company guidelines that govern the handling of personal data are to be brought to employees' attention. The instruction must be documented in writing or in another form. Furthermore, every employee can access additional information on the Data Protection and Privacy Office portal page.

SAP Global Human Resources is responsible for providing the instruction.

c. Employees

It is the duty of all SAP employees to treat personal data to which they have access in the course of fulfilling their contractual duties with SAP as confidential.

SAP employees may collect, process, and/or use personal data only to the extent required to fulfill their duties, and in accordance with approved processes. If collecting, processing, or using personal data is not recognizably prohibited for the employee, he or she can refer to the legality of the management's instructions. In case of doubt, employees may contact the DPPO for clarification (mail: privacy@sap.com).

5. Details

a. Notification, Accuracy of Data, and Inspection

A person affected must be informed in a suitable manner that their personal data is being collected, processed, and/or used. Usually, they are to be informed before the time at which data is collected.

The person affected must be informed of the SAP company collecting the data, the purpose for collecting, processing, or using the data, as well as other recipients to whom their data will be transferred. The information must be provided in a way that is easy to understand.

Stored personal data must be accurate. Inaccurate data must be corrected or deleted as soon as practicably possible. All processes for collecting, processing, and/or using personal data must contain an option for correcting, updating, and, where required by applicable law, deleting or blocking.

A person affected may, at any time, request information about the data stored on them, its origin, purpose for storing, and recipients to whom the data is passed on. Queries or complaints submitted by a person affected must be processed by the SAP company responsible without undue delay or according to those timeframes imposed by local law, whichever is the earlier. Objections from a person affected with regard to the processing of personal data must be investigated and, if necessary, remedial action must be taken.

b. Duration of Storage, Data Deletion

For every process in which personal data is collected, processed, or used, a schedule must be defined for the regular deletion of personal data after the specified purpose has been fulfilled or if the legal basis no longer applies.

Instead of deleting the personal data, it may also be irreversibly anonymized, meaning retained in such a way that makes it no longer possible to identify individual persons. If, for technical or legal reasons (for example, if the retention of data is legally required for tax purposes), it is not possible to either delete or anonymize personal data, this personal data must be blocked for any further processing and/or use, as well as for further access.

c. Additional Rules for Special Types of Personal Data

Special types of personal data are details on racial and ethnic origin, political views, religious or philosophical beliefs, union membership, health, or sexual preferences. Special types of personal data are equal to such personal data that requires special sensitivity for the persons affected (sensitive data). For example, this is the case for data on criminal activities, as well as on those individuals who in their respective country fall below the age legally deemed as adult i.e. minors.

In the instances in which SAP, or third parties acting on behalf of SAP, collect special types of personal data, management must ensure that the persons affected have been informed in advance and have given their consent for this. Provided that applicable law does not determine otherwise, special types of personal data may be collected,

stored, processed, and transferred only with the explicit consent of the persons affected. Increased precautions (for example, physical safety features, encryption, and access restrictions) that are appropriate for the special sensitivity are to be taken for collecting, storing, processing, and transferring this data.

The following additional rules apply for these special categories of data:

- The collection, processing, and/or use of this data must be transparent for the persons affected at all times.
- Consent given by persons affected must refer explicitly to these special categories of data.
- Processes that involve collecting or using special types of personal data may be configured only with a prior check performed by the DPPO, or in consultation with the local DPPC.

d. Transfer of personal data/Commissioned Data Processing

If personal data is to be exchanged within the SAP Group or with other companies, it must first be checked whether contractual agreements on data protection and privacy and data security are required. Such a check is always required if an SAP Group company is to process data on behalf of another SAP Group company, or if an external service provider is to process data on behalf of an SAP company ("transfer for processing purposes"). A check is also necessary if an SAP Group company transfers data to another SAP Group company or an external company (for example, a service provider, partner, or customer), and the receiving company wishes to use the data for its own business purposes ("transfer for own purposes"). The legally compliant transfer of personal data within the SAP Group is ensured based on internal company commissioned data processing agreements (intra-group data transfer agreements or an 'IGA').

If personal data under SAP's legal responsibility is transferred to an SAP company located in the European Union or in Switzerland, Liechtenstein, Iceland, or Norway, or in a country not mentioned, it must also be ensured in advance that a suitable level of protection in accordance with Articles 25 and 26 of the EU Data Protection Directive (95/46/EC) is guaranteed.

If personal data is transferred, the following rules apply:

Transfer for commissioned processing:

The SAP company that commissions or instructs another SAP company or an external company to collect, process, or store personal data is responsible for compliance with the requirements of data protection and privacy regulations. This responsibility does not cease with the transfer to the other SAP or external company.

Every SAP company must ensure that external companies who are to collect, process, or store personal data on their behalf, are reviewed in advance and then regularly to ensure that they comply with the requirements of data protection and privacy regulations, and that the necessary contracts with these companies have been concluded. The review can be delegated to central units within the SAP Group. A regular review also takes place within the companies of the SAP Group.

Transfer for recipient's own purposes:

The transfer of personal data to another company within the SAP Group or an external company for their own purposes is allowed only if this is permitted or required by law, or if the persons affected have given their prior consent. The transferring SAP company must ensure that the legal requirements are checked before the data is transferred.

Transfer to state agencies (authorities and courts):

SAP will transfer personal data to governmental agencies only on the basis of applicable law and after the DPPO and Global Legal have performed a prior check, and taking into account other required areas within the SAP Group.

In the event of a request for information from a governmental authority or a court of competent jurisdiction, SAP will inform the person affected of this without undue delay.

6. Transfer of Customer Data

SAP processes customer personal data. This means not only the personal data of a customer's employees/business partners etc. but also the personal data belonging to SAP's customer's own customers. The transfer and use of such customer data must be performed in full compliance with applicable law and those additional obligations agreed in the contract between us. Personal data of customers may never be passed on to third parties without an appropriate legal or contractual basis.

In this respect, SAP works with its customers to support them in complying with the applicable data protection and privacy legislation; however, this does not include providing our customers with any legal advice or giving them any guarantee that their legal compliance with data protection and privacy laws are guaranteed.

7. Data Protection and Privacy Supervisory Authorities

If so required by law, contract and/or the obligations set down in this Policy, SAP companies must always cooperate with any data protection and privacy supervisory authority irrespective of whether such authoritative entity is based within the EEA or outside the EEA.

If a data protection and privacy supervisory authority requests information or otherwise exercises their right of investigation, the DPPO must be informed without delay (mail: privacy@sap.com). The DPPO shall then act as primary coordinator to formulate an appropriate response to the query in consultation with the other responsible departments (for example, Global Legal, Legal Compliance & Integrity, IT Security, Global GRC), and acts as a direct contact person with the respective data protection and privacy supervisory authorities.

8. Data Protection and Privacy and Data Security

Certain data protection and privacy laws require special security measures to be implemented when collecting, processing, and/or using personal data. SAP shall define such measures in compliance with the legal requirements in the SAP Security Policy and the related Security Standards and Guidelines. The DPPO shall assist in defining and updating these standards and guidelines.

9. Data Protection and Privacy Organization

a. Position of the Data Protection Officer and Global Organization

The DPPO is an appointed organizational unit within SAP SE. It reports directly to the responsible board member and is managed by the SAP SE Data Protection Officer.

The DPPO determines the SAP Group's data protection and privacy strategy in accordance with the strategic objectives of the SAP Group and ensures that the SAP Group companies adhere to the applicable provisions of the data protection and privacy regulations. The DPPO is to be supported in performing its tasks. In particular, the DPPO is to be provided with the resources required to perform its tasks and is to be provided with any requested information fully and without undue delay.

The Data Protection Officer is free to exercise his/her tasks as they see fit. The DPPO employees are only bound by the instructions of the Data Protection Officer. The Data Protection Officer and the DPPO employees must not be discriminated against for performing their tasks.

The DPPO maintains a network of data protection and privacy coordinators, who, in accordance with section 9b of this Policy, are to be appointed by the respective SAP companies and central organizations. The tasks of the global organization are defined in Annex 1. The DPPCs are to be supported by their respective SAP companies in performing their tasks and must not be discriminated against for performing their tasks.

b. Organization at Local, Regional, and Line-of-Business Level

This obligation is broken down into 2 key subsections, as follows:

(1) It is the duty of every SAP company to appoint a DPPC for their business unit, and to inform the DPPO the name of the the personnel appointed. More than one SAP company can also appoint the same DPPC jointly.

All DPPCs must have a direct functional reporting line to the head of the relevant SAP unit to which they have been appointed. They must ensure compliance with relevant data protection and privacy laws and the provisions of this Policy. They shall regularly align their activities with the DPPO, but are otherwise free to exercise their expertise in the area of data protection and privacy as they see fit, and must not be discriminated against for performing their tasks.

The appointment as DPPC can only be revoked in agreement with the SAP SE Data Protection Officer. If a DPPC's appointment comes to an end or is otherwise terminated, the respective SAP company must appoint a new DPPC in good time and inform the DPPO.

The respective business units to which the DPPCs are appointed shall provide the DPPCs with reasonable time to work required by the DPPC to administer its DPPC duties and suitable resources shall be allocated to the DPPC in order for them to perform its tasks. To ensure that the DPPC retains and benefits from learning resources to ensure the necessary expertise to fulfil their duties, they shall be permitted to participate in further education and professional development funded by SAP upon mutual agreement with their managers.

A DPPC shall undertake those tasks outlined at Annex 2. In the event of any query regarding the nature and scope of such tasks, the DPPC (or manager responsible for the DPPC) may contact the DPPO for further clarification.

(2) Organizations and/or business units of an SAP company who do not in their daily tasks administer personal data are also, at the request of the DPPO, obliged to appoint a DPPC responsible for the respective organization. Accordingly, the provisions of section 9b (1) apply to the DPPCs.

10. Data Protection and Privacy Standards

The requirements under this Policy can be specified and enhanced through data protection and privacy standards. Such data protection and privacy standards may only come into effect after the DPPO has reviewed and approved their compatibility with this Policy.

11. Raising Awareness

The DPPO and DPPCs shall take measures to raise awareness at regular intervals. All employees and third parties acting on behalf of SAP are regularly informed about both their duties and their rights within the scope of this Policy and applicable laws.

A.3 Greenhost Terms and Conditions

Greenhost Usage Terms and Conditions

Terms and Conditions

These general terms and conditions apply to all offers and agreements between Greenhost B.V. Amsterdam, Chamber of Commerce 62576593 (“Greenhost”) and its counter parties (“Customer”). Terms or conditions set by customer that deviate from or do not appear in these general terms and conditions are only binding for Greenhost if it has been agreed upon explicitly in writing.

Article 1. Offer and acceptance

1.1. Customer can make a selection via the Greenhost site from the various packages of services, such as web hosting, mediation for registration of domain names, provision of SSL certificates, installation of software for virtual servers (the “Services”) that Greenhost is willing to deliver. Exclusively on the website described package description of the Services is binding.
1.2. If Customer makes a selection of desired services via another channel (such as telephone, letter or in person) , Greenhost will make a quotation of the services required, the prices and how these services are delivered.
1.3. The submitted selection from paragraph 1 or the acceptance of the quotation from paragraph 2 leads to an agreement between Greenhost and Client at the time of its receipt by Greenhost. Greenhost will Customer a confirmation e-mail received. Customer can until the time of receipt of this email cancel the agreement.
1.4. If Customer is a natural person not acting in the exercise of profession or business, Customer may, within seven days after completion of the agreement terminate this by notifying Greenhost. This right lapses as soon as a Customer Service time or Greenhost permission to do work on behalf of a Service. The law does not exist in mediating registration of domain names, as it always is performed immediately after application and with the consent of Customer.
1.5. All changes in the implementation of a Service at Customer’s request are considered additional work when it added cost considered additional work and as a result less work when there is less cost. The same applies when a change in circumstances, a different implementation is required. Greenhost may adjust the prices accordingly unilaterally, but only after consultation with Customer.

Article 2. Implementation of the Services

2.1. After the conclusion of the agreement as soon as possible Greenhost will provide the Services in accordance with the agreement, taking into account reasonable further wishes of Customer. Greenhost guarantees that the Services to the best can be performed using due care and workmanship. The following applies to delivery times are indicative unless otherwise indicated.
2.3. If and insofar as the proper implementation of the Services requires, Greenhost has the right to commission certain activities by third parties. These third parties operate under the responsibility and supervision of Greenhost.
2.4. Customer will already do all that is reasonably necessary and desirable to allow a timely and proper execution of the agreement. In particular contributes Customer ensure that all business and data which Greenhost indicates are necessary or which the Client reasonably understand to be necessary to provide the Services will be provided to Greenhost.
2.5. Greenhost has the right to provide the Services to suspend or restrict supply if it turns out that the Customer in respect of the contract an obligation to Greenhost not come after or acts in violation of these terms or the law.
2.6. Customer shall at entering into the agreement a working email address to give up. Greenhost may send all

communications concerning the agreement to this email address. This email address should work throughout the contract. If the change email address, Customer must notify the change from this email address. Requests for information or access to customer data should also be done from this email address.
2.7. Greenhost focuses on energy saving, “green” hosting and other services. As used Greenhost only renewable energy sources. Greenhost strive to improve in this area with its service. The ISO 26000 standard for social responsibility of organizations is leading in this.

Article 3. Support by Greenhost

3.1. Greenhost will remain available for a reasonable level of remote support by phone or email. The times of availability and any response times will be published or will be communicated manner to be agreed on the website of Greenhost.
3.2. Greenhost will the necessary software (like VPS environments, Apache, MySQL, etc.) install and / or configure on systems managed by Greenhost.
3.3. Additional software must be installed by the Customer himself. Customer will ensure that this software up to date, particularly with regard to security. On request Greenhost can be of help, which Greenhost entitled to charge its usual hourly rate. If Greenhost finds that Customer does not properly update the security software Greenhost can intervene in accordance with Article 5.
3.4. If necessary for the use of software licenses from third parties, Customer will decrease these licenses and ensure that its provisions are strictly complied with. On request Greenhost may decrease certain licenses and transfer to the Customer, against mutually agreed fee. Customer indemnifies Greenhost claims by third parties relating to installation and licensing of software, except insofar as the claims are the result of information or licenses are delivered by Greenhost.
3.5. When Customer believes that software does not work or not adequate (eg. A low performance) Greenhost is ready to examine this further and propose a plan for improvement. To conduct of the study and the improvement charges are applicable, unless it appears that the cause of failure or not working properly due to Greenhost itself.

Article 4. Availability of systems

4.1. If a Service (partly) supplied through systems and / or networks managed by Greenhost, such as web hosting, e-mail transmission / reception or access to online software or management tools, Greenhost will endeavor in this Service to uninterrupted availability of these systems and to create networks and to realize access to data stored by Greenhost.
4.2. Greenhost does not guarantee the continuous availability, unless otherwise agreed by means of a so-called Service Level Agreement.
4.3. Greenhost will endeavor to keep the systems it uses and software up to date. Greenhost here is however dependent on its supplier (s). Greenhost is entitled to install an update or postpone patch until they can test it has been adequately and evaluate.
4.4. If access to an administrative account and / or a management agreed so to come Customer may be agreed aspects of managing the Service, Greenhost will provide the Customer with an administrative username and password. Every action that occurs via the administrative account or an account of an individual user of the Customer is considered to be under the responsibility and risk of the Customer. In cases of suspected abuse of an account Customer must report this as soon as possible so that Greenhost can take these measures.
4.5. Greenhost will make regular backups of Customer’s systems of Greenhost stored data for continuity purposes. These backups are not made available to Customer only by Greenhost used for data recovery to continuity problems. The provision of the backups or individual files from it is possible only in special cases and upon payment of the then current standard rate.
4.6. If the backup service as agreed Greenhost will provide the created backup to Customer for unmediated

access.
4.7. Customer's obligation to meet the agreed limits for data transfer, storage and / or processing capacity. Exceeding is Greenhost authorized further use to restrict or block the Service, or to bring an additional amount in accordance with the then applicable amounts for additional processor capacity, data transfer or storage. Greenhost will warn the customer in time before bringing additional used capiciteit charged.

Article 5. Rules of conduct on content

5.1. Customer may not store or distribute information in violation of the law or the terms and conditions.
5.2. In particular, Customer may not store or distribute information that
offense involves forms of pornography or libelous, defamatory, racist, discriminatory, hateful,
infringes the rights of third parties, in any case, but not limited to copyrights, trademark rights and portrait rights,
contains unsolicited commercial, charitable or philanthropic communication.
5.3. It is prohibited to store or transmit data or processes or software, whether through the systems of Greenhost boot which Customer knows or can reasonably suspect that this Greenhost, other users of the Services or Internet users or damage can inflict.
5.4. Greenhost can logs and maintain records of the use of the Services in order to measure the performance of its systems and to identify violations of this article. Greenhost will however not keep logs on individual outbound email traffic without special permission from the Customer.
5.5. If in the opinion of Greenhost has been a violation of this article, Greenhost is entitled to take all measures it deems reasonably necessary to terminate or reduce the impact. These measures are elaborated in the "notice and takedown" policy as stated on the Greenhost website. This will include the lock may or disabling access to information or disabling software. Greenhost will notify Customer of any action under this Article. If Greenhost costs must make to end a violation or to minimize the impact, it will be recovered from the Client.
5.6. When sufficiently plausible that there is a wrongful act against a third party and that third party has a real interest in the issue of personal data of Customer or any user of a Service, Greenhost is also entitled to this data to make these third available. Greenhost in this situation will create a balance of interests and if feasible Customer prior notice of its intention. State the procedure to be worked out in the Notice-Takedown Policy Greenhost and transparent for each customer.

Article 6. Experimental Software

6.1. Greenhost may make available certain software as an experiment as a service. The Customer is free here or not to use.
6.2. If Customer chooses to use this software, Customer understands and agrees that, that the software is experimental and without any warranty or claim to function properly or be available is offered.
6.3. Greenhost may at any time and without further modification to extend the experimental software, modify or discontinue the supply thereof. For this, no liability is accepted regardless of how long the software is available and if Customer has announced that he will continue to use the experimental software.
6.4. On request, experimental software included as part of a Service. In that case no longer applies the provisions of this Article. Greenhost will in that case before a quote for the cost of this issue, which Customer must approve to the experimental software part of a Service.

Article 7. Domain names, IP addresses and SSL certificates

7.1. Application, allocation and possible use of a domain name, IP address and / or SSL certificate depend on and are subject to the rules and procedures of the registering authorities, such as the Foundation for Internet Domain Registration in the Netherlands or the issuing certification authority. The relevant authority decides on the

allocation. Greenhost performs the application only an intermediary role and does not guarantee that a request will be honored.
7.2. Greenhost is entitled to charge for the mediation service and the service of the commissioning of the domain name, IP address and SSL certificate administration. These are notified in advance.
7.3. Only the confirmation of Greenhost, stating that a domain name, IP address and / or SSL certificate has been issued, or its commissioning on behalf of a Service, is proof of grant. A bill of Greenhost application or mediation is not a confirmation of registration.
7.4. Greenhost will ensure that domain names assigned by Customer through Greenhost, IP addresses and / or SSL certificates for services usable and available in accordance with Article 4. Customer indemnifies and holds Greenhost harmless for all damages related to (the use of) domain name, IP address and / or SSL certificate by or on behalf of Customer.
7.5. Greenhost is not liable for the losses caused by Customer of his right (s) on a domain, IP address and / or SSL certificate, or the fact that a domain name or IP address is acquired by a third party and / or obtained, subject in case of intent or deliberate recklessness of Greenhost.
7.6. Unless otherwise agreed, only deployed an IP address for the duration of the agreement on behalf of Customer. IP addresses can be shared with other clients of Greenhost, unless the nature of the service does not allow or desirable. Customer may not claim an IP address or take unless expressly agreed in writing. Furthermore Greenhost entitled to change IP addresses as necessary for a good supply of the Service (s).

Article 8. Intellectual property rights

8.1. All intellectual property rights at all in the context of a service made available to work (such as software, scripts, texts or images) are held exclusively by Greenhost or its suppliers. Customer acquires only the user rights and responsibilities arising from the scope of the agreement or granted in writing and the Customer will work not reproduce or publish.
8.2. If any intellectual property right is transferred to a work of Greenhost to Customer, Greenhost retains an unlimited and perpetual license to use the work and its components in its business operations and deliver to others. This does not affect the duty of Greenhost to confidential customer information confidential.
8.3. All rights of use of works made available expire upon termination or rescission of the contract.

Article 9. Prices and payment

9.1. Customer shall pay annually in advance the amount of Greenhost. Variable amounts must be met monthly in arrears Greenhost. Greenhost will send a bill for the amount owed by the Customer to Customer. Greenhost sends electronic invoices unless otherwise agreed.
9.2. If Customer believes that (part of) an invoice is incorrect, he must report this within the payment to Host Green. The payment of the disputed (but not otherwise) shall be suspended until Greenhost investigated the report. If Greenhost after study concludes that the complaint was unjustified, Customer shall within seven days to pay the disputed yet.
9.3. The invoice of Greenhost is 14 days after the invoice date. In a late payment, Customer, in addition to the amount due and the interest due thereon, held to a full compensation of both judicial and extrajudicial collection costs, including costs for lawyers, bailiffs and debt collection agencies.
5.5. 9.4. Greenhost is entitled to adjust the rates charged once per calendar year. Greenhost will Client of this at least 2 (two) months inform in advance. Customer with a price the right to terminate the contract at the time it enters into force.

Article 10. Confidentiality

10.1. Parties will information they before, during or after the execution of the agreement provide to each other as confidential if this information is marked as confidential or if the receiving party knows or should reasonably suspect that the information was intended as confidential. Parties also impose this obligation on their employees and third parties engaged by them to implement the agreement.
10.2. Greenhost will not take cognizance of data recorded by Customer and / or distributed through the systems managed by Greenhost, unless the Customer's consent, access has been necessary for the proper performance of the contract or Greenhost is required to do so under a statutory provision or authorized order by the authorities. In that case Greenhost will endeavor cognizance of the data to minimize, to the extent within its power and, if possible, inform the customer of this application up to date.
10.3. Greenhost reserves the right at all times increased by the implementation of the agreement to use knowledge for other clients, provided that no information of the Customer in breach of obligations of confidentiality is made available to third parties.
10.4. The obligations of this article which remain after the termination of the Agreement for any reason, and so much for so long as the providing party can reasonably claim to the confidentiality of the information.

Article 11. Liability

11.1. Greenhost is only liable to Customer in the event of a culpable breach of the agreement and only for compensatory damages, ie compensation for the value of the omitted performance.
11.2. Any liability of Greenhost is excluded for any other form of damage, including among other things, additional compensation in any form whatsoever, compensation for indirect or consequential damages, loss of revenues or profits, damages for loss of data and damage for exceeding terms due to changed circumstances.
11.3. The maximum amount that can be paid in case of liability under paragraph 1 which is billed for the six months preceding the month in which the damage occurred. This maximum amount will lapse if and insofar as the damage is caused by intent or gross negligence of Greenhost.
11.4. The liability of Greenhost due to culpable breach of contract arises only if Customer Greenhost immediately and properly be in default, stating a reasonable period to remedy the deficiency, and Greenhost after that period attributable to fulfill its obligations deficit continues to shoot. The notice must contain a detailed description of the failure, so Greenhost is able to respond adequately.
11.5. In case of force majeure, ie every event which fulfillment of the agreement can not reasonably be demanded of Greenhost, the implementation of the agreement will be suspended or terminate the agreement if the force majeure situation has lasted longer than sixty days, all without any liability for damages.

Article 12. Term and Termination

12.1. This agreement is valid for a minimum period of one year, unless otherwise agreed in writing. The agreement can only be terminated prematurely as provided in these Terms and Conditions, or by mutual consent.
12.2. The agreement is in the absence of a written notice in good time for a thirty day notice period is automatically renewed for a period of one year.
12.3. If Customer is a consumer, in derogation of the previous paragraph, the contract after the minimum term into a contract of indefinite duration. Customer can always cancel the contract with a notice period of one month. Notice thereof can through the same channel through which Customer has notified the acceptance, as well as in writing or via the control panel or administrative account (if any).
12.4. Upon cancellation referred to in the previous paragraph Greenhost will refund any paid but become unduly by termination amounts forward.

Article 13. Amendments to Agreement

13.1. After acceptance, the contract may only be amended by mutual consent.
13.2. Greenhost is once per calendar entitled these terms to unilaterally modify or expand. They must do so at least thirty days before the modifications or extensions effect will be to give notice to the Customer.
13.3. If the Customer within this period objector Greenhost will consider whether the objectionable changes or expansions wish to withdraw or not. It will make its decision notice to Customer. If Greenhost objectionable modifications or extensions not to revoke, the Customer has the right to terminate the agreement as of the date that this impact will be.
13.4. Greenhost may make changes at any time in these conditions if they are necessary because of revised legislation. Against such changes, Customer may not object.

Article 14. Final Provisions

14.1. This agreement is governed by Dutch law. Insofar as the mandatory law does not otherwise, all disputes that may arise as a result of this agreement will be submitted to the competent Dutch court for the district in which Greenhost is located.
14.2. If any provision is found to be void under this contract, this will not affect the validity of the entire agreement. The parties shall in that case, replace (a) new provision (s), which as far as legally possible to the intent of the original agreement and these terms and conditions will be reflected.
14.3. “In writing” in these conditions also email and fax communication, provided the identity of the sender and the integrity of the contents sufficiently established. The parties will endeavor to confirm receipt and content of communication by e-mail.
14.4. Received by Greenhost or saved version of any communication shall be deemed authentic, subject to proof to the contrary by the Client.
14.5. Each party is only entitled to assign its rights and obligations under the contract to a third party without the written consent of the other party. However: Greenhost always be entitled to assign its rights and obligations under the contract to a parent, subsidiary or affiliated company.

A.4 Mobile Vikings Terms and Conditions

Privacy conditions

The explanation of the information we collect from you.

Definities

In these Privacy Conditions following terms are used.

- "VikingCo NV" indicates VikingCo NV;
- "Services" indicate the services offered for sale on this Website;
- "Information" indicates the information concerning the visitors to this Website, as described in article 4;
- "VikingCo NV" / "us" indicates the VikingCo NV, Kempische Steenweg 309/1, B-3500 Hasselt; email address: info@vikingco.com ; V.A.T.: BE 0886.946.917;
- "Products" indicate the services and products mentionned on this Website;
- "Website" indicates the website of Mobile Vikings on the URL www.vikingco.com or any other URL that leads to the same content.

Introduction

VikingCo NV strives to offer the highest possible standard of service to its customers. To be able to guarantee this quality, VikingCo NV needs to collect certain information about you. In this respect, VikingCo NV commits itself to protect your privacy and to follow the guidelines from the Law issued on December 8, 1992 (“Wet van 8 december 1992 tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens”).

Your Permission

1. By using this WebSite you agree with these Privacy Conditions and the way information can be collected and used by VikingCo NV, as with the possible transfer of this information, as described below.

2. We are allowed to change these conditions in the future. In that case we will announce the changed conditions on the Website.

Information Collecting

1. When you register, we need to collect certain information to complete the registration. This infomation will be part of a permanent file regarding your transactions with VikingCo NV. This file contains primarily following data: first name, last name, address, email address, date of birth, phonenumber.
2. It is possible that – when sending us an email – we will request certain information from you in order to be able to respond quickly and correctly to your questions, or to verify the data of your permanent file. This information may be included in our permanent file concerning you.
3. When contacting us, by any means, it is possible that we, if necessary, include certain remarks with respect to this contact in your permanent file. This allows us to offer a better service to our customer.

Cookies

1. The Website uses cookies to improve your experience when browsing the website. No sensitive personal data is stored in these cookies, and the Website will remain fully functional when disabling cookies in your browser.
2. From time to time VikingCo NV will use marketing agencies to insure our publicity on the Internet. These companies use cookies to measure the effectiveness of the publicity. For this purpose these companies may use information regarding your visit to this or other websites. Unless otherwise stated, no names, addresses, email addresses or phone numbers or used. No connection is made between internet usage or cookies and identifiable persons.
3. You can disable cookies during your visit to the website. More information regarding cookies can be found at www.allaboutcookies.org.

Usage and transfer of information

1. You agree that we and carefully selected others can contact you from time to time using email, telephone, SMS or MMS regarding products or services that we believe could be of interest to you.
2. You agree that VikingCo NV may send you emails and newsletters from time to time with following contents: information about VikingCo NV products and services. At any time, you have the right to ask VikingCo NV to stop sending these emails and newsletters.
3. You agree that VikingCo NV uses this information for the following purposes:
    1. Handling your orders and requests, managing bills and invoices, processing invoices of service providers, managing questions, requests or complaints, legal procedures or any other administrative or commercial activity;
    2. Conducting market research to inform you about our products and services, new features or improvements of products or services, special offers, discounts and prices that VikingCo NV deems relevant;
    3. Giving information according to legal, administrative or regulatory rules applying to VikingCo NV or relating to legal disputes, fraude, criminal acts or the prosecution of (alleged) forgers or relating to credit requests coming from the User.
    4. Performing activities relating to the management of VikingCo NV, like staff training, quality control, network management, testing and maintaining computers and other systems and relating the transfer of a part of VikingCo NV.

Right to access

1. On request and without any additional costs, you have the right to oppose the use of your private information for purposes of direct marketing. You can inform us of this by sending a letter to the following address:
   VikingCo NV, Kempische Steenweg 309/1, B-3500 Hasselt, Belgium or by sending an e-mail to info@vikingco.com
2. On simple request you have the right to access your personal information for free, and the right to correct it. Please contact us on the (email) address mentioned above if you wish to verify, change or alter your data.