ENSURESEC Data Protection Policy

# **Data Protection Policy for raising campaign**

## **ENSURESEC – Data Protection Policy for awareness raising campaign**

### **What is ENSURESEC**

ENSURESEC is a security solution which protects e-commerce operations from cyber and physical threats. In order to do this, it **monitors** the whole e-commerce operation, from browsing to delivery. It **identifies** cyber and physical threats, and **responds to** and **mitigates** those threats. The ENSURESEC project is a project funded and under the supervision of the European Commission, in order to develop and test the ENSURESEC solution.

### **Why your personal data might be involved and processed by ENSURESEC?[[1]](#footnote-1)**

During the research activities and the rollout of the project, personal information will be inevitably processed. In such case, if your personal data are processed, you will be the ‘**data subject**’. Hereby we sum up under what circumstance we process your personal data.

### **Data Processing for awareness raising campaign**

Besides ENSURESE core research on technologies to improve the cybersecurity of the European e-commerce ecosystem, awareness raising campaign are run in order to improve the general knowledge of e-commerce customer regarding cybersecurity. To this end, personal data, such as names, email address, phone numbers imight be collected and processed.

### **The Controller**

According to the GDPR (Article 4), ‘controller’ *means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*; In substance, the controller is the person or entity which leads the personal data processing operation by determining purposes and means for the processing.

In ENSURESEC, processing operations are handled by different partners. However, supervision over such operations and the determination of purposes and means are dealt with by the responsible partners in close coordination with the entity responsible for the project (i.e., project coordinator). Below the contact points of the project coordinator, should you have any query regarding the way personal data is processed:

INOV – Instituto de Engenharia de Sistemas e Computadores Inovação

Rua Alves Redol, 9
1000-029 Lisboa

Email: ensuresec@inov.pt

## **How the project processes personal data**

### **Legal Basis**

The legal basis for processing your personal data for this ENSURESEC pilot study is your consent, in accordance with Article 6(1) of the GDPR. As the participation to our pilot study is entirely voluntary, we rely on your consent to process your personal data. According to Art. 7(3) of the GDPR, you have the right to withdraw your consent at any time. Please read this Data Protection Policy in its entirety, before deciding whether you would like to consent or not.

### **Some information on the policy of the project and about the ways personal data are processed**

Processing personal information pursuing research interests implies that a number of safeguards and proactive initiatives are taken in order to protect your data protection rights. In order to do so, ENSURESEC project partners begin all processing of personal data by following these principles:

* **Fairness and lawfulness**. Personal data are processed fairly and for the purposes for which they were collected initially. Moreover, personal data processing operations are assessed against their legality by the project coordinator.
* **Security of processing**. Personal data processing operations are conducted following the available security measures, both technical and organizational. As an example, access control and authentication-based environments are applied to the access to data-sets containing personal data, and the need-to-know principle is implemented in the vetting of any researcher involved in ENSURESEC personal data processing operation.
* **Minimization**. Collection and processing of personal data, including during the technology testing and the data storage, follow the principle of data minimization. This means, for example, collecting your data in a way that only the strictly necessary amount of it is processed. Furthermore, whenever personal details will be needed, pseudonymization will be sought.
* **Third-party non-disclosure**. No personal data will be disclosed to any third-party (i.e. non-consortium entities) unless there is an explicit authorization to do so by the interested individual or a contractual obligation to be fulfilled. Such a situation may occur for auditing purposes.
* **Use-case-based access**. Personal data will remain within the consortium domain. Furthermore, personal data will only be accessed by the partners with an involvement in the use-case you are asked to participate. If the partner does not have any interest or involvement in a use case, personal data processed therein will not be disclosed to them, in accordance to the need-to-know principle.
* **Long-term identification is not an aim**. It is not in the purposes of this project to retain personal data for long periods and to aggregate such data so to identify you. When personal data are processed for research finalities, such sets will mostly be operated for the duration of the testing and immediately deleted afterwards, unless otherwise indicated.
* **Accuracy**. ENSURESEC project regularly reviews datasets where personal data are stored in order to ensure the accuracy and reliability of the information therein. Systems to update the information are in place so to ensure both security and controlled access to datasets.

## **For how long we will keep your data?**

If immediate deletion will not occur, that means we have a legal obligation and/or a research purpose to archive the data either for contractual reasons or for scientific research finalities. In such case, ENSURESEC partners will keep your personal data in question for a maximum of 1 year after the termination of the project, unless otherwise indicated or requested by a supervisory authority or for auditing purposes.

## **Your rights concerning the personal data we process**

If you, as a data subject, believe that any of your personal data are processed by ENSURESEC, you are entitled to request the controller to undertake the following actions:

* **Right to access**. You are entitled to request information regarding your personal data, including purposes, categories of information, recipients, retention, source of collection, transfer to third-countries (non-EU Member States). Moreover, the data subject is entitled to receive a copy of such data.
* **Erasure or rectification**. You may request at any time for their personal data to be amended, updated or erased by the controller. If the input you have provided has already been included in the research result, it might no longer be possible to retrieve and destroy that data.
* **Restriction of processing**. You have the right to request that your data are suspended from being processed, anytime the data results to be inaccurate or unlawfully or unnecessarily processed.
* **Object.** You have the right to object to the processing of your personal data anytime they demonstrate grounds relating their particular situation.
* **Automated decision-making or profiling.** Data subjects have the right not to be subjects to automated decision making processes (including profiling) which substantiates in legal consequences for him or her.

## **Who you can address your questions to?**

ENSURESEC contact point is the following:

INOV – Instituto de Engenharia de Sistemas e Computadores Inovação

Rua Alves Redol, 9
1000-029 Lisboa

Email: ensuresec.coordination@inov.pt

## **Remedies**

ENSURESEC Consortium is committed to timely respond to any inquiry you may have, and reasonably comply with any exercise of your rights enlisted above. However, you should be aware that, each time your requests are not satisfactorily fulfilled by the controller, or you believe that your rights have been violated, recourse to data protection authorities or to the ordinary judicial branch is still possible.

## **How we embed privacy and data protection within the consortium**

ENSURESEC project values the respect for privacy and data protection as both a legal requirement and an ethical standard. For this reason, we indicate below the periodical actions and initiatives we undertake in order to frequently review the way the project observes and respects privacy standards.

**1. Respect for GDPR and its obligations in the scientific research domain.** The main legal act we rely upon for complying with privacy and data protection rights is the GDPR. In this respect, we continuously assess our activities, particularly if or when involving personal data processing operations for scientific research purposes, against the rights of the individuals and our legal obligations enshrined in the GDPR.

**2. Accountability**. We maintain and regularly update internal policies enabling the consortium to keep records and documentation of the relevant personal data processing operations. These actions include the assessment of the risks that our research may occur to the rights and freedoms of individuals. Such processes aim at identifying mitigation measures and enabling safeguards against data protection and privacy violation, and are recorded in the so-called DPIA (data protection impact assessment).

**3. Awareness raising.** We regularly undertake activities aimed at informing our consortium partners about the data protection obligations and standards that we abide to. Initiatives are performed on a periodical basis and include webinars, presentations and ad-hoc sessions on privacy, data protection and the respect for fundamental rights in research activities. Privacy sessions are organized in the course of general assemblies organized by the consortium.

**4. Ethical standards.** As mentioned above, we do not only regard the protection of personal data and privacy as a legal requirement to meet. ENSURESEC project considers personal data protection obligations as an ethical standard of best practice, in line with H2020 principles. For this reason, the consortium implements and assesses privacy beyond what imposed by law and as a by-design principle, including in the development of any technology and its integration within use-case scenarios.

**5. Further research guidelines**. ENSURESEC project makes extensive use as a benchmark and as a code of conduct of further ethical guidelines issued by the European Commission on responsible research. Such manuals inform researchers and projects funded under the Horizon2020 and similar EU funding programs about the best practices to be adopted when the research involves the processing of personal data.

1. In this policy, we use the following terms:

Controller (see definition below)

Data subject: sometimes we refer to ‘data subject’ and ‘you’ interchangeably. [↑](#footnote-ref-1)