Data Protection Policy Template for companies offering CT Smart Home owner services, as data controllers

The present data protection policy clarifies in a layered manner the processing of personal information of users of the Cyber-Trust Smart Home owner services, as part of *[describe offer]* or independently as separate service. The data processing occurring by the Cyber-Trust services is pursuant to the provision of the EU General Data Protection Regulation (GDPR) and the e-Privacy Directive (with the reservation of the national implementing and transposing laws), and in accordance with the country-specific data protection regime applicable to *COMPANY* offering the Cyber-Trust Smart Home owner services. For further information, please check Section 2 of the present data protection policy.

Hereinafter, by using the terms "we" and "our"; we refer to the data controller (*COMPANY*). Hereinafter, by using the terms "you" and "your", we refer to the Smart Home owner user.

This document will provide you with information about the policies covering all the operations which involve to some extent processing of your personal data. Personal data, as defined in Article 4(1) General Data Protection Regulation (GDPR) include any information relating to an identified or identifiable living natural person. Personal data can be your first name, last name, e-mail address, email format, IP address and so forth. The e-Privacy Directive and the respective national acts further protect the confidentiality of your communications, including the installment on your equipment of agents which are authorized only for specific reasons to collect and process specific information.

The contents of this policy can be seen below:

1. About our company

Please insert here information about the data controller.

2. About Cyber-Trust

2.1. What is Cyber-Trust?

Cyber-Trust is a research project that has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme, H2020-DS-SC7-2017, under grant agreement no. 786698. The project started on 1 May 2018 and ends on 31 April 2021. The Cyber-Trust consortium consists of nine partners from academia, consultancy and business. The Cyber-Trust consortium

designed, developed and built the Smart Home owner services to allow Smart Home owners, as part of a contract with a telecommunications service provider, to safeguard their Home and devices.

2.2. Smart Home owner services

The Cyber-Trust platform provides a variety of services. The Smart Home owner services constitute one of the offered platform services, used by *COMPANY* to offer enhanced security solutions to Smart Home owners.

The Cyber-Trust platform has been built with data protection by design in mind. All the services process the minimum amount of personal data by default, unless explicitly requested by the Smart Owner to be provided with a service which requires a higher-intensity data processing level.

Specifically, the Smart Home owner services include the provision of:

- Advanced detection of cyber-threats with the latest techniques
- Intelligent response mechanisms preventing attacks from succeeding
- Informative messages about how trusted a device should be considered
- Informative messages about the devices presenting some risk
- Sophisticated attack log collection with tamper resistance storage
- Full parametrization of the defensive mechanisms to the users' needs
- Important notifications about ongoing cyber-security incidents

3. Contact information of the data controller and of the Data Protection Officer

Please insert here the information of the COMPANY
Please insert here the information of the Data Protection Officer of the COMPANY
The contact information of the Cyber-Trust is NAME and email address.

4. Personal Data we process via the Cyber-Trust Smart Home owner service for the provision of the service *(to be configured)*

Type of data	**What data we process**	**Purpose**	**Legal basis**	**Data retention period**
Account and billing data	• Email address • Phone number • Full name (first name, last name) • Username • Date of birtth • masked credit card number • product license information • user preferences	• To authenticate you; • To separate one end-user from other end-users with same name; • To send you notifications or important information about the service. • To send you communications regarding your license and support • To manage your account and facilitate your	• Consent • Contract	As long as necessary for the provision of the service requested by you and in line with our legal obligations, and in any case no longer than [depends on country]

		login into the service • To know until when your account is valid • To know what type of services you wish to receive from Cyber-Trust and under what conditions		
Device data	Information about: • Operating system • hardware and firmware from device manufacturer • city/country of device • error logs • browser • network (network transactions, list of running processes and list of network interfaces) • applications running on the device	• To provide you with the requested service • To create device profiles in order to detect abnormalities • To provide an assessment of the devices' trust level, to be used in the context of cyber-defence • To construct the attack graph and assess the security status of your smart home	• Consent • Contract	As long as necessary for the provision of the service requested by you and in line with our legal obligations, and in any case no longer than [depends on country]
Other Service data	Information about: • malware samples and malware detections • URLs of websites • IP addresses • usage statistics (activation, crashes, scans, errors)	• To provide you with the requested service; • To construct the attack graph and assess the security status of your smart home.	• Consent • Contract • Legitimate interest	As long as necessary for the provision of the service requested by you and in line with our legal obligations, and in any case no longer than [depends on country]

	• *More information may be included*			

5. Explanation of our legal basis for the different types of data processing

When the data processing is based on consent: The processing of certain data may require your consent (Article 6(1)(a) GDPR in conjunction with Article 7 GDPR). In that case, you will be informed and you will be provided with the opportunity to allow such processing or not. You will always have the option to revoke your consent for future processing.

When the data processing is necessary for contract initiation and performance: We primarily process personal data needed to fulfill our contractual obligations to you ((Article 6(1)(b) GDPR), which are to protect your smart infrastructure and data against malware and attacks. Thus, depending on the requested service, our contractual obligations will include the monitoring of various internal and external data streams, programs, and files, to the minimum extent possible and strictly necessary for the provision of the requested service. You will have the option to choose between lower and higher-intensity processing operations, as well as the frequency of alerts you would like to receive in order to confirm a proposed action.

When the data processing is based on our legitimate interest: We may process data on the basis of our legitimate interest (Article 6(1)(f)). In that case, we are obliged to disclose our legitimate interest.

- If personal data supplied by third parties is processed, part of the processing is carried out on the contractual basis and part of the processing according to Article 6(1)(f) GDPR. In the latter case, our legitimate interest is the protection of your smart infrastructure.
- If processing is necessary for the protection of our own infrastructure and service *(for telecommunication providers*), the processing is carried out on the basis of our legitimate interests. In that case, our legitimate interest is the protection of our services to you to ensure availability and continuance and the protection of our overall infrastructure. In specific cases, it is our obligation to take, at our own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of those services.

You have the right to object to the processing insofar as there are reasons for this arising from your particular situation.

You can find information about all your rights under *Your rights*.

6. Disclosure of your data

In order to provide you with the requested services, in order to safeguard your infrastructure from active or future security threats and in order to ensure that our services are continuously available and secure, there will be occasions where we or our partners (on our behalf) will have to transmit specific categories of personal data to third parties. This will be done exclusively on the following legal bases *[Please further specify, wherever necessary]*:

- *based on your express consent;*
- *for the performance of our contractual obligations towards you;*
- *based on a legal obligation;*
- *based on our legitimate interest, when there is no overriding legitimate interest in the non-disclosure of your data;*

The recipients of the data are *[Please further specify, wherever necessary, by providing a list of the third-party recipients, including data processors]*:

- *Employees (internal and external)*
- *Data processors who provide us with services and process the data on our behalf (IT infrastructure service providers, Payment processors, Software service providers, etc)*
- *Public authorities, including Law Enforcement Agencies.*

7. Your rights

As a data subject, you have the following rights:

- pursuant to Article 7(3) GDPR, to withdraw your consent at any time and without any consequences for you. This means that in future we may no longer continue to process the data as based on this consent;
- pursuant to Article 15 GDPR, to obtain information about whether your personal data are processed by us and where that is the case, access to those personal data. In particular, you may obtain information about the purpose of processing, the category of the personal data, the categories of recipients, to whom your data has been or is disclosed to, the storage period planned, the existence of a right to request from the controller rectification, erasure, restriction of processing or objection, the existence of a right to lodge a complaint and the source of your data if it has not been collected by us. Pursuant to Article 12, we must provide any communication relating to the processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- pursuant to Article 16 GDPR, to obtain the rectification of inaccurate personal data without undue delay or the completion of your personal data stored with us;
- pursuant to Article 17 GDPR, to obtain the erasure of your personal data stored with us unless processing is necessary to exercise the right to freedom of expression and information, for compliance with a legal obligation, for reasons of public interest, or to establish, exercise or defend legal claims;
- pursuant to Article 18 GDPR, to obtain the restriction of the processing of your personal data;
- pursuant to Article 20 GDPR, to receive your personal data, in a structured, commonly used and machine-readable format or to obtain the transmission to another data controller (right to data portability);
- pursuant to Article 21 GDPR, to object, on grounds relating from your particular situation, at any time to processing of your personal data, which is based on data processing for the purposes of legitimate interests. If you file an objection, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or unless processing serves the establishment, exercise or defence of legal claims.
- pursuant to Article 77 GDPR, to lodge a complaint with a national supervisory authority. You can contact the supervisory authority of your habitual residence or workplace or our company headquarters. In the latter case, you can file a complaint with the respective National Supervisory Authority.
- If you wish to exercise any of your rights, please see 2. Contact information of the data controller and the Data Protection Officer.

8. Your preferences for the processing of your data

You can make certain choices about how your data are used by us by adjusting the privacy settings of the relevant service we provide to you.

9. Technical and organisational measures

Cyber-Trust has implemented high-quality safeguards to protect your personal data. Those safeguards include state-of-the-art solutions which meet the requirements of data protection legislation. Cyber-Trust reviews and regularly updates those measures, in order to protect your data against accidental or

intentional manipulation, partial or total loss, destruction or unauthorized obtaining, or access by third parties.

Moreover, Cyber-Trust implements measures to protect its own systems and infrastructure. These include data encryption, pseudonymization and anonymization as well as logical and physical access restriction and firewalls.

Please insert here COMPANY's technical and organisational measures, for instance regular trainings for employees, confidentiality controls, integrity tests, etc.

10. Section for US users based on California Privacy Laws

You can see all the categories, sources and purposes of collected personal information, listed in the section *Personal Data We Process*.

You can see how your data are disclosed to other third-party recipients under the section *Disclosure of your data.*

You have the right to:

- know what personal information is being collected about you;
- know whether your personal information is sold or disclosed and to whom;
- say no to the sale of personal information (right to opt out);
- request erasure of your personal information; information will be deleted if no exception applies (including our right to defend our lawful interests);
- access your personal information; specific information shall be provided in a portable and, to the extent technically feasible, in a readily useable format but not more than twice in a 12-month period;
- equal service and price, even if you exercise your privacy rights.

Under California Civil Code § 1798.83, the consumers must receive the following information upon written request: a. the categories of personal information that we have disclosed to third parties within the prior year, if that information was subsequently used for marketing purposes; and b. the names and addresses of all such third parties to whom such personal information was disclosed.

For further information, please feel free to submit your request to the contacts found under *Contact information of the data controller and of the Data Protection Officer*.

11. Amendments to this Data Protection Policy

This data protection policy is effective as of *Date*.
We - in cooperation with our partners - keep our Data Protection Policy under regular review to make sure it is up to date and precise. Thus, it may become necessary to change it due to the potential addition of new features to the Cyber-Trust Smart Home owner services. Every time our Data Protection Policy is reviewed, you will receive a notification and you will be given sufficient time, to decide whether you wish to continue using the Cyber-Trust Smart Home owner services.