

Privacy statement for customers and service providers of itrust consulting s.à r.l. (ITR-PrivacyStatCust)

1 General information

Last updated	18/06/2024
Our commitment	Respecting everyone's privacy is the objective of the itrust consulting, which is committed to ensuring the protection of your personal data. itrust consulting wishes to inform you in full transparency on the way it collects, uses and protects your personal data (hereafter called PII, personal identifiable information) and implements adequate means to ensure the protection of your data and compliance with the requirements.
What does this statement cover?	This privacy statement applies to all PII transmitted to itrust consulting and to PII which itrust consulting processes in the course of its activities. It does not cover data of employees.
Who is responsible for your data?	The company itrust consulting is responsible for your PII and ensures compliance with the regulations. You can contact itrust consulting or its Managing Director under: Carlo Harpes, info@itrust.lu , +352 26 17 62 12. Additionally, itrust consulting has appointed a data protection officer (DPO) to assist you in executing your rights.
DPO contact	Guillaume Schaff, dpo@itrust.lu , +352 621 699 975.
How to change these rules?	itrust consulting may change this privacy statement by posting an updated version on our website.

2 Principles at itrust consulting

itrust consulting attributes great importance to the protection of PII. This is confirmed by the implementation of a data protection policy specific to itrust consulting.

The approach of itrust consulting is based on six principles:

1. itrust consulting always uses your PII in a fair and trustworthy manner.
2. It is committed to take all appropriate technical and organizational measures to protect the security of your PII and especially the confidentiality, integrity and availability of your PII.
3. You have the right to be informed about how your PII is used. itrust consulting will be transparent to you about the data that is collected and how it is used.
4. If you are unsure about how your PII is processed, please contact us so that we can answer your questions as soon as possible.
5. All necessary measures are taken to protect your information against misuse and to keep it secure.
6. itrust consulting cooperates with the Commission Nationale pour la Protection des Données (hereinafter, the CNPD), having its registered office at L-4361 Esch-sur-Alzette, 1 avenue du Rock'n'roll.

3 Rules of conduct at itrust consulting

3.1 What is the mission of itrust consulting?

Your PII is used solely within the framework of the mission of itrust consulting, which is specialising in Information Security Systems, helping its customers from both the public and private sectors protect their information against any divulgation, manipulation, or unavailability. It consists in offering services related to:

- building, implementing, and auditing Information Security Management Systems,
- assessing and treating risk with its own TRICK Service tool,
- deploying security experts whenever needed (SECaaS, or Security as a Service),
- on request hacking of our customers and handling cybersecurity incidents (malware.lu CERT), or
- designing and operating security solutions for ICT.

You will find more details under <http://www.itrust.lu>.

3.2 What are the purposes of the treatments?

The collection and processing of your PII is limited to the following purposes:

- To manage data according to contract (consulting, audit, training, research, ...).
- To assign login names or pseudonyms to student performing standardised tests; to provide access to the link to teacher supervising the test and providing feedback to students.
- To translate sets of student names with similar properties in classes of pseudonyms to perform statistical correlation of test results with that properties, without revealing the identity of test participants.
- To demonstrate the quality of work or identify errors in case of complaint (by the customer or stakeholders).

- To reuse know-how applied on one customer for another.
- To document the history of InfoSec and CyberSec in Luxembourg.
- To document the history of InfoSec and CyberSec in Luxembourg.
- To propose general and tailored services, to enrol customers by establishing contracts, to change contracts.
- To invoice customers and follow-up payments and project closure.
- To manage staff actions on all IT systems.
- To ensure IT Systems Security.
- To contract people and operate a safe workplace.
- To manage and pay salaries and social security fees.
- To manage accounting information according to legal requirement.
- To prepare or support internal management decisions.
- To assist customers with forensic analysis and event response team activities
- To host malware database, malware testing tools and manage technical knowledge related to malware.
- To simplify navigation on the website.
- To ensure IT Systems Security, i.e., to prove that no one touched ICT systems of itrust.
- To investigate manipulations.

3.3 Who is concerned by data processing?

The following are concerned:

- all customers, in particular customer's staff interacting with itrust consulting;
- all contractual partners and subcontractors;
- students and teachers affected by the management of ÉpStan;
- all employees of itrust consulting.

3.4 How is your PII collected?

Concerning the persons mentioned in point 3.3, data are collected from

1. information you give us directly;
2. information that we may collect via our browsing activities on our websites itrust.lu and malware.lu., and we may collect on sources like LinkedIn, twitter, etc.;
3. Database managing ÉpStan.

3.5 What PII does itrust consulting have at its disposal?

'PII' means information that identifies you or makes you identifiable. This may include in particular:

- your name, address, identifiers, profile image, email address, and telephone number;
- electronic information (IP address, browsing information);
- other information about your past or current business activities and also information including PII which you may transmit to us;

- employee evaluations;
- information related to disciplinary measures.

3.6 How long is the data retained?

Your personal data is kept for the time necessary to achieve the above-mentioned purposes.

These periods may, however, be increased by the need to apply statutory limitation periods. The retention periods have been defined in the record of processing activities and can be consulted on the premises of itrust consulting. Alternately a concise table from record of processing is Table 1: Retention time from record of processing activities. The customers' data are retained during all the period of services with itrust consulting. For any question about the time retention of your PII, you can contact our DPO.

Depending on the purpose or provisions of the archiving laws, the retention period could be extended. Indeed, some images are kept and used for historical purposes.

In anonymised form, your personal data may be used for statistical purposes beyond the above-mentioned retention period.

Knowledge management for the provision of business services and management of customer data in record or processing is as below:

Type of data	Retention time	Deletion time after request
Spare PII as evidence in consulting or audit mission.	10 years from the closure off the social year except in case of existing legal litigation to civil court 30 years (for commercial it is only 10 years after social year closure of the final court decision.	1 month.
Paper documents related to customer.	3y after end of project.	2 months
Login and activity reports (related to activities of customer staff, e.g. Owncloud changes, app.trickservice logins, MS Teams conference...	10 y (This is a maximum; depending on systems, logs are deleted faster or in case of upgrades, e.g. in MS Team, log are deleted according to MS policies.)	2 months
IT Logs	5y (Max)	2 months
Some customer reports (that were not subject to deletion request) may be kept for scientific and journalistic purposes, e.g. the first malware incident discussed in the LU Parliament, the first 27001 Gab analysis in the public sector...)	30y	2 months

Table 1: Retention time from record of processing activities for management of customer data

3.7 With whom is your PII shared?

As a general rule, your personal data is not shared outside itrust consulting. Access to your data will only be granted to those persons working at itrust consulting who need it for the performance of their duties.

In the context of investigations by other authorities (e.g. police investigation), itrust consulting may be required to provide them with the information necessary for their investigation.

In the case of participation in events, we pass on the necessary data to the organisers with your consent.

If we process your data, you can send an email to the DPO to find out more about our list of processors.

3.8 Are your PII transferred to third countries (outside the EU and partner countries)?

None of your PII is transferred to organisations outside the EU.

3.9 How is your PII protected?

Access to your PII is restricted to prevent unauthorised access, modifications or misuse. Access is granted only to those members of staff who need it for the performance of their duties.

3.10 How itrust consulting manages cookies

A cookie is a text file sent to your browser and stored on the hard drive of your device (e.g. PC, laptop or smartphone) when you visit our website.

itrust consulting uses different types of cookies. Session or preference cookies, which are essential for navigation and the proper functioning of the site. Cookies for audience measurement to track the following information about visitors. The purpose of these cookies is to measure the number of users of the services. Cookies for statistical purposes to track how users browse our site. itrust uses the Matomo solution, configured according to the recommendations of the EDPB to comply with the GDPR. These cookies do not contain any personal data.

itrust consulting keeps the data collected by the cookies by storing them in the data servers that belong to itrust consulting and that are located at itrust consulting's head office. The data is stored in Europe.

Cookies set by our website can only read by it. itrust consulting doesn't use an external service to analyse how people are using its site.

We use cookies to evaluate the functionality of our website and to collect data to create statistics to improve quality. You can accept or decline our cookies (only statistics cookies). A default "no consent" option applies in case you have not chosen. If you choose to decline our cookies, we will not install statistics cookies, as functional cookies are always installed automatically. If you would like to know more about our cookie policy, please click on the link in the right lower corner on our website to 'Change Cookie Settings'.

3.11 What are your rights and how do you exercise them?

The legal rules on the protection of PII, in particular the rights of the data subjects concerned by the processing operations carried out are applicable under the relevant conditions and subject to the exceptions and derogations provided for.

For questions relating to the processing of your data or in order to exercise your rights, you may contact the Data Protection Officer of itrust consulting,

- by sending an email to the following address: dpo@itrust.lu.
- or by registered mail to

itrust consulting s.à r.l.
Data Protection Officer
G. Schaff
55, rue Gabriel Lippmann
L-6947 Niederanven, LUXEMBOURG

while enclosing with your application a legible and valid copy of your identity document and, if applicable, that of the person for whom you are the legal representative.

If you have any questions, you can also contact the person who carried out the data processing directly.

You have the right to:

1. request a copy of the PII that itrust consulting holds about you;
2. ask itrust consulting to correct, update, or delete your PII from its files, and
3. to report any misuse of your PII.

In the event of a request for deletion of your data, itrust consulting will check that there are no other purposes or rights of another data subject that would oblige it to keep them. In this case, the decision should be notified.

If you request a copy of your file, itrust consulting will analyse it in order to delete any information on other persons.

If you believe that your personal data have not been processed in accordance with the law, you have the right to contact the CNPD (www.cnpd.lu) or to lodge a complaint with them.

19/06/2024

X 

Carlo Harpes
Managing director
Signed by: Carlo Harpes