

DATA PROTECTION POLICY

VERSION 18 MAY 2021

1 - Introduction

This document sets out Kyos responsibilities and policy for privacy and the protection of personally identifiable information (PII). Service provider in the field of IT security, personal data protection of our customers, suppliers and employees is an important issue at Kyos. Because we are concerned about your questions regarding our internal policy on the subject and because transparency is a value we hold dear, we have drawn up this data protection policy, detailing the measures adopted at KYOS regarding the processing of personal data that we may collect as a result of our activity.

2 – Regulatory Context

2.1 – Personal Data Protection in Switzerland

KYOS is a limited company and a Swiss nationality with its headquarters in Geneva, it is subject to the Federal law on Data Protection Act (FDPA).

2.2 – Personal Data Protection in European Union

The General Data Protection Regulation (“GDPR”) n°2016/679 is a European regulation applicable since 25 May 2018 to all Member States of the European Union. It aims to protect the privacy of individuals by imposing measures relating to each stage of the life cycle of a data. This regulation also provides for administrative sanctions and/or fines in case of failure to comply with these rules.

KYOS’ Swiss nationality does not prevent it from complying with the GDPR as a processor (see paragraph 2.2) of its European customers.

For information, a personal data is any information relating to a natural person that allows that person to be identified or made identifiable.

3 Kyos and personal data protection

3-1 Controller and processor

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.

Processor means the natural or legal person, public authority, agency, or body which process personal data on behalf of the controller.

3-2 Presentation of Kyos in its roles as controller and processor

KYOS acts almost exclusively as a processor of personal data of its customers.

KYOS also acts as a data controller for its internal organization, i.e. in relation to its employees, by collecting their personal data in the context of their employment contracts.

4 – Compliance

4.1 – Privacy by design/ by default

In application of the principle of privacy by design, Kyos undertakes to implement the issue of personal data protection from the conception of a processing operation, in particular by

collecting only the personal data strictly necessary for the purpose of the planned processing.

Kyos also undertakes to ensure the highest level of protection by default, i.e. to systematically implement security and protection measures in the event of processing involving personal data, in accordance with the principle of privacy by default.

4.2 – Information security policy

Aware of the role that trust play in our activity, Kyos is implementing an information security policy based on Information Security Management System (ISMS) with a view to obtaining ISO27001 certification in 2021.

4.3 – Trusted Partner

Kyos is concerned with the values that we hold and that we wish to promote in the exercise of our activity, and we are concerned with the same requirement with regard to our suppliers. Over the years, we have surrounded ourselves with trusted partners with whom we share common values such as transparency and respect.

You can find the list of our partners on the Kyos website: www.kyos.ch

4.4 – Data transfers outside the European Union

In the course of providing its services, Kyos may transfer personal data to the European, which is in line with Swiss data protection regulations.

Furthermore, by using cloud services whose data is hosted in Switzerland and Europe, or by having implemented organizational and technical measures that are also adequate to the GDPR and the FDPA, your data is processed securely as required by the applicable regulations.

Any request for the transfer of personal data beyond the European Union is subject to authorization of the data protection advisor after assessment of the risks involved.

4.5 – Retention period

Kyos only retains the personal data collected for as long as is necessary for the purposes of the processing in accordance with the principles of data minimization and limitation.

4.6 – Awareness and training

Because security depends on everyone, Kyos employees are made aware of the cyber risks so that they can adopt the right actions on a daily basis. Our employees are also made aware of the issues surrounding personal data, for example by drawing up an information note for employees defining the subject and informing them of the rights regarding the protection of personal data.

4.7 – Data breach

A personal data breach is defined by the GDPR (article 4.12) as “a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed”.

Because there is no such thing as a zero risk, if a personal data breach or more generally a security incident were to occur, Kyos has established an incident management policy, describing the steps to be taken in the event of such an event occurring.

This procedure aims firstly to stop the incident in question as quickly as possible and to find the cause in order to best protect our customers, suppliers, employees, and other people concerned. It also aims to find out what steps to take in terms of communicating the incident according to the impact it may have on the rights and freedoms of individuals.

4.7.1 - As a data controller

When acting as a data controller, Kyos undertakes to document internally, in its breach register; the nature of the breach, if possible, the categories and approximate number of persons affected by the breach, the categories and approximate number of personal data records affected, a description of the likely consequences of the data breach, the measures taken or foreseeable to prevent a recurrence of the incident or to mitigate the possible negative consequences.

4.7.2 - As a processor

When Kyos acts as a processor, it undertakes to inform the controller of any breach of which it is the victim and of which it is aware. It also undertakes to provide the controller with all the information at its disposal in order to best assist the controller in dealing with the breach.

4.8 – Individual rights

4.8.1 - Description of rights and procedure

As data subjects remain the owners of their personal data, the GDPR lists the rights that any data subject can assert against the controller.

Any request relating to these individual rights should be sent to the Data Protection Advisor by:

- Email: privacy@kyos.ch
- Post: Kyos SA, Chemin Frank-Thomas, 32, 1208 Geneva

The Data Protection Advisor has a maximum of one month to respond to the request.

If the request is complex or if the number of requests is too high, the response time may be extended up to two months, provided that the person(s) concerned are informed of this extension during the first month. If there is any doubt about the identity of the person making the request, the data protection officer may ask him or her to provide proof of identity, for example by requesting an official document.

For information, the individual rights are the following:

- The right to be informed (Art 13 GDPR): the data subject has the right to be informed of the purpose of the collection of information and whether it is obligatory or voluntary, the recipients of the information, his/her rights, and possible transfers of the data to a country outside the European Union.
- The right of access (Art 15 GDPR): the data subject has the right to obtain from the controller confirmation as to whether or not personal data relation to him or her are being processed and, where they are, access to such data.
- The right of rectification (Art 16 GDPR): the data subject has the right to obtain from the controller the rectification of personal data relating to him or her which are inaccurate or to complete incomplete information by means of a supplementary statement.
- The right to portability (Art 20 GDPR): concerns only personal data processed on the legal basis of consent and contractual performance. The data subject has the right to receive the personal data concerning him or her that he or she provided to a controller in a structured, commonly used, and machine-readable format, and has the right to transmit that data to

another controller without the controller to whom the personal data have been communicated having to object.

- The right to erasure (Art 17 GDPR): the data subject has the right to obtain from the controller the erasure of personal data concerning him or her.
- The right to object (Art 21 GDPR): the data subject has the right to object at any time, on grounds relating to his or her particular situation, to the processing of personal data concerning him or her.
- The right to data restriction (Art 18 GDPR): the data subject has the right to request a temporary freeze on the concerning of some his/her data.

4.8.2 - Kyos commitments as a processor

As a processor, Kyos undertakes to send to the controller any information necessary for the exercise of these rights and to forward any request in this regard to the relevant controller.

4.9 Policy review

This data protection policy shall be kept up to date after any reform in the field of personal data protection or after any internal changes affecting this document.