AGENTIL

Data Protection Declaration

November 27th 2024

Version 1.1

1. Introduction

AGENTIL SA (hereinafter: AGENTIL) attaches great importance to responsible and legally compliant processing of personal data. The processing of personal data is carried out solely on the basis of applicable law.

In this data protection declaration, we inform our customers as well as visitors to our websites (hereinafter: customers) about the collection, storage and processing of personal data.

We process data only on the basis of applicable law. Data processing is subject to the new Federal Data Protection Law (nLPD) and the ordinances relating to the New Federal Data Protection Law (OnLPD).

Consulting our websites from abroad may also be subject to foreign data protection laws.

AGENTIL reserves the right to modify this data protection declaration at any time. The version in force is that published at the address: www.agentil.com.

This data protection declaration describes our practices and consists of the following chapters:

- The data collection
- Data
- Treatments
- Protective measures
- The organization

2. Data Collection

We collect and process data that is necessary for our business, for example:

• Personal data (surname, first name, position, address, etc.)

• Professional contact data (telephone, email address, etc.)

• Company data (all data linked to your company and your employees, data from your software package, etc.)

• Financial data (account relationships, your bank details, your credit insurer reference, your payments, etc.)

• Identification data (e.g. cookies, IP addresses, etc.),

• Location data (already mentioned on the website, etc.)

• Image-related data (video or written testimonials from our clients, SEO, etc.)

• Etc.

We distinguish several ways in which this data is requested.

2.1. Provided:

All the data that you make available to us during your visits to our websites and the use of registration forms.

2.2. Collected :

All data that we collect on request, for example when concluding a contract. For the proper management of our commercial relationship, we request a set of specific information or reference documents.

2.3. Received: via third parties (partners / suppliers)

All data concerning you that we receive from trusted third parties, in particular during procedures linked to solvency checks.

2.4. Automatic

All data collected by Cookies, monitoring, etc.

2.5. The Consent

Before any data collection action, AGENTIL respects the notion of prior consent. By consent we mean: “any manifestation of free, specific, informed and unambiguous will by which a data subject accepts, by a declaration or by a clear positive act, that personal data concerning him or her are subject to collection and treatment".

2.6. Rights

2.6.1. The right of access

The data subject has the right to obtain from the controller confirmation that his or her personal and/or sensitive data are or are not being processed and, where they are, he or she has the right to obtain access to said data as well as some additional information. This right also includes the right to obtain a copy of the data that is being processed.

2.6.2. The right of rectification

The data subject has the right to request that their data be rectified or completed as soon as possible.

2.6.3. The right of erasure or « right to be forgotten »

The data subject has the right to request erasure of their data as soon as possible. If the data of the data subject has been transmitted to other entities, the “right to be forgotten” mechanism is triggered: the data controller must take all reasonable measures to inform the other entities that the data subject has requested the erasure of any link to their personal and/or sensitive data, or any copy or reproduction thereof.

Subject to compliance with obligations relating to legal data retention periods (see article 8.1.4).

3. Data

AGENTIL processes the personal data of its customers who are in direct or indirect contact with it. We use the term “data” synonymously with the term “personal data”. Data is information that relates directly to a customer or that we can attribute directly to a customer.

In section 3.2, AGENTIL informs about the categories of data processed in accordance with the information contained in this data protection declaration.

When data relating to other persons is communicated to us, the sender confirms that he is authorized to do so and that the data is correct. Before providing us with this data, the sender must ensure that the third parties in question are aware that we are processing their data.

This data protection declaration therefore applies to data that we have already collected or will collect in the future.

3.1. What data is processed ?

Depending on the situation and purpose, we process various personal data from different sources. We collect and obtain this data primarily directly from our customers, particularly when establishing contractual relationships, when they use our products and services or as part of general communications.

We may also obtain data from other sources, for example from public registers or other publicly accessible sources, from authorities or any other third parties. In this context, AGENTIL processes different categories of data. The main categories of data are described below:

3.1.1. Basic Data:

Master data is data relating to identity as well as situation and characteristics, such as name, address or date of birth. This data may also relate to third parties (proxy holders) and also includes signing rights, powers of attorney and declarations of consent.

3.1.2. Contractual Data:

When a contract is concluded with us, we process, in addition to the basic data, other data, such as information on the purchase and use of products and services. This data includes information about the processing and execution of contracts as well as feedback from our customers regarding the services.

3.1.3. Communication Data:

Communication data is data relating to communication with our customers, whether this communication takes place in the form of exchange of letters, by telephone or through electronic channels (e.g. via e-mail, SMS etc.).). They also include authentication data (e.g. authentication data, biometric data, etc.) as well as video and audio recordings. When verifying your identity (e.g. in the event of an enquiry), we additionally collect data in order to identify you (e.g. by means of a copy of an identification document).

3.1.4. Technical Data:

• Technical data is data that we collect when using one of our electronic services. This data also includes the IP address of a device and logs in which we record the use of our systems.

• To ensure that these offers work, we may assign an individual code to the terminals (e.g. in the form of a cookie). Technical data does not allow conclusions to be drawn about the identity of a person.

• By combining them with data from user accounts, registrations, access controls or contract execution, we can, where appropriate, associate other data with natural persons.

3.1.5. Registrastion Data:

Registration data is data about customers that is transmitted during registration or activation in order to use or participate in certain offers and services (e.g. newsletters and forms).

3.1.6. Other data:

We collect other customer data in different contexts. Thus, data is collected in the context of administrative or judicial procedures (e.g. documents, means of proof, etc.). We may also collect data for fraud prevention purposes.

3.2. Data Type – Definitions

3.2.1. Personal data: identification

Personal data refers to any information that allows a moral or legal person to be identified and a unambiguous relationship to be established.

This may include information such as name, address, telephone number, email address, IP address, social security number, credit card number, etc.

For example, in the context of a business, personal data could be the information of employees, customers or business partners.

3.2.2. Private data: strong identification

Private data refers to personal information that is not available to the general public and is considered private to a specific person or entity.

This may include data of a financial nature, such as bank statements, bank account numbers, credit card data, medical information, legal records, personal information, etc. For example, a company's private data could include internal financial information, confidential contracts, unpublished research and development reports, etc.

3.2.3. Sensitive data: profiling

Sensitive data is a subcategory of private data that requires enhanced protection due to its extremely confidential nature.

This data is considered particularly sensitive because its disclosure or misuse could cause serious harm to an individual or organization.

Common examples of sensitive data include medical or mental health information, genetic data, political or religious opinions, sexual orientations, ethnic or racial origins, biometric data, etc.

In the context of a business, sensitive data can be patent information, trade secrets, future product plans, national security information, etc.

3.3. Impact Analysis

For the impact analysis of personal data stored on our systems, we use an impact analysis tool: PIA (Privacy Impat Assesment), Data Protection Impact Analysis (AIPD).

https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

The PIA software is part of an approach to supporting data controllers in implementing the obligations of the nLPD. It allows and supports the conduct of an impact analysis relating to data protection, which is mandatory for certain processing operations.

3.4. Data retention time

3.4.1. Data hosted on our BCS:

We delete personal data from our database two (2) weeks after the contract ends. The saved data is deleted one (1) month after the data is deleted from the database.

3.4.2. Data present in our ERP:

Customer accounts are switched to “inactive” status because it is not possible for us to completely delete the data for reasons of control and integrity of systems and archives.

3.4.3. Data present on our marketing materials:

The data used and distributed on our marketing content are governed by a distribution authorization signed by the client which is valid for 3 years from the date of signature, this agreement must be renewed upon expiry so that AGENTIL can continue to use those data. The customer can request their deletion at any time.

3.4.4. Data stored locally:

Data stored locally is only kept for the time necessary for processing. Each customer can request its deletion at any time.

3.5. Date and scope

This data protection declaration applies from the moment personal and/or sensitive data becomes known to us.

This data protection declaration applies to all processes during which we process your data, in particular when:

- Consultation of our website

- Contact us

- Pre-sales process, demonstrations or sales meetings,

- Contractual process (placing an order for products and/or services, invoicing, payment)

- Product and/or service delivery process,

- Process of dissemination of documents, information or communications from us,

- Marketing process,

- Recruitment process,

- Etc.

4. Treatments

Processing means any operation relating to data, for example collection, storage, use, disclosure or erasure.

This data protection declaration describes how we process data when customers use our services or products, relate to us under a contract or communicate with us generally.

This data protection declaration therefore applies to the processing of data that we have already collected or will collect in the future.

We inform separately about certain data processing, for example in other data protection notices, in T&Cs, in descriptions of products and services, on our websites, in declarations of consent, contracts and notices forms.

4.1. Responsibilities

AGENTIL is responsible for data processing in accordance with this data protection declaration; it is also the competent service in matters of data protection, unless otherwise indicated in a particular case.

To exercise your rights and contact us for any questions regarding the protection of personal data, you can contact us:

• in writing to the following address: AGENTIL SA, Data Protection, Rue du Pré-de-la-Fontaine 19, 1242 Satigny - GE,

• by e-mail: dpo@agentil.com,

• by telephone on +41 (0)22 595 04 04.

4.2. Objectives / purposes

The purpose of this declaration is to inform you transparently about the use of your data. We use your data to:

4.2.1. Conclude / Execute a contract :

As part of the contractual relationship, we carry out all the processing necessary for the preparation, conclusion, execution or implementation of the contract. Before concluding a contract, we inquire about your creditworthiness (information about your ability to pay and your payment conduct), in order to determine whether we can actually conclude the contract and, if so, in what form. To deliver ordered goods

to you, we may transmit your data to a third-party service provider (e.g. the Post Office). In addition, for payment transactions, we exchange your data with a financial service provider.

4.2.2. Communicate:

As part of customer relations, we exchange information (contract, documents, etc.) for the performance of our services, the improvement of our services, etc.

This is the case when you fill out one of our contact forms, when you contact us by email, by post, by telephone or by another means or when we contact you. For this purpose, we process in particular the following data (personal and/or sensitive, contact, financial data). We may do anything necessary to communicate with you, including responding to your requests or contacting you if we have any questions.

We draw your attention to the fact that we randomly record telephone communications or video conferences for reasons of quality improvement or proof (certification, audit, etc.) or at the express request of the customer.

4.2.3. Marketing and sales actions:

As part of a marketing campaign or SEO action, we process information allowing us to inform you about our offers in an appropriate manner. We may send you information and offers by post or electronic means (newsletters, emails, or other electronic messages and the postal mailing of advertising brochures, magazines or other printed matter, etc.), making you share of product or service recommendations.

We may give you vouchers or invite you to events, draws and competitions.

We personalize these offers and information using the data you give us.

4.2.4. Comply with legal requirements:

In connection with this, we are obliged to comply with legal requirements and, in the event of violations, to cooperate with the authorities.

This is the case when it comes to applying the provisions relating to all the laws to which we are subject (GDPR, nLPD, Data Protection Act, etc.) and compliance with other regulatory requirements (Certification , audit, etc.).

We may be, in the context of the prevention and explanation of criminal acts or misconduct, required to transmit information or documents to the authorities or collaborate in investigations carried out by authorities (e.g. criminal prosecutions or supervisory authority, etc.).

4.2.5. Other purposes:

As part of our internal processes and administration, we may use your personal data.

This is the case for operations carried out for administrative and statistical purposes as well as the evaluation and improvement of our internal processes.

4.3. Treatment locality

Your data is processed in Switzerland, France, Europe or outside these geographic areas. Always via secure channels.

5. Protective Measures

5.1. Access

Who has access to your data at AGENTIL and to whom do we transmit it?

5.1.1. AGENTIL Employees:

Our organization defines precise roles, responsibilities and profiles for each of the activities of our employees (finance, administration, sales, etc.). In this context, we define the rules allowing access to your data and the type of authorized processing. These rules are monitored and reviewed on a regular basis and may be modified at any time.

5.1.2. AGENTIL Partners:

As part of the relationship with certain partners (publishers, subcontractors, etc.) we are required to transmit certain data. For example when processing an order requiring the name of the end user to be entered (license management).

When hosting data on our Cloud, our partner is subject to the same data protection rules and requirements.

In all cases, AGENTIL controls its correct application.

We have verified compliance with this requirement with our suppliers and partners.

Each partner or subcontractor is required to sign a mutual confidentiality agreement as well as a commitment to respect data protection law.

5.2. Process

5.2.1. Control of subcontractors

We verify compliance with this requirement with our suppliers and partners on the basis of an inspection.

5.2.2. Explicit Consent

AGENTIL asks you for explicit consent from the start of the exchanges because we attach fundamental importance to the explicit consent of all our customers for the collection of their personal data.

In accordance with the principles set out by the nLPD, consent must be free, specific, informed and unequivocal. It is essential that we obtain clear and affirmative authorization from you, in order to guarantee transparency and respect for your privacy.

5.2.3. Raising awareness among AGENTIL employees

Our employees are made aware of the protection of the data they are required to process and undertake to respect rules, principles and duties, in particular through staff regulations, regular communications and an IT charter detailing best practices.

5.3. Software solutions

5.3.1. PIA (see article 3.3)

5.3.2. 2FA

We use a double authentication tool for access control to our systems.

5.3.3. Safe PW

We use a password management tool for creating, tracking, updating, storing.

5.3.4. Anti-virus

We use antivirus for all of our systems, this antivirus is regularly checked and updated by the person responsible for administering our systems.

5.3.5. Anonymization

We regularly anonymize personal data whenever we are required to transmit data to third parties.

5.4. Hardware Solutions

5.4.1. Private Hosting

Selection of a certified professional Datacenter. The Datacenter which hosts the data of customers who have chosen our BCS solution meets all the optimal conditions in terms of data protection and is certified according to the standards in force. Certifications and additional information are available on our website.

6. Organization

6.1. Processing Manager

Taking into account the nature, scope, context and purposes of the processing as well as the risks, the degree of probability and severity of which vary, for the rights and freedoms of physical persons, the controller implements measures appropriate technical and organizational measures to ensure and be able to demonstrate that the processing is carried out in accordance with the legislation.

These measures are reviewed and updated if necessary.

6.2. Data Protection Officer

A Data Protection Officer has been appointed to ensure the reception of possible requests concerning the data processed and to provide a response.

He/She is also responsible for communicating and interacting with the authorities responsible for data protection.

This delegate can be reached at dpo@agentil.com.

6.3. IT Security Manager

He/She is responsible for managing software and hardware solutions and more particularly related updates.

6.4. Financial Direction

He/She is responsible for assigning access rights to financial data.

6.5. Human Resources Department

He/She is responsible for granting access rights to personal data.

7. Data Breach Notification

7.1. Breach Description

A data breach occurs when the data for which we are responsible experiences a security incident that results in a breach of confidentiality, availability, or integrity.

7.2. Notification deadline

If the breach poses a risk to the rights and freedoms of an individual, we will notify the competent supervisory authority as soon as possible, and at the latest within 72 hours of becoming aware of the breach.

If the data breach poses a high risk to affected individuals, they will also be informed as soon as possible after becoming aware of the breach, unless effective technical and organizational safeguards or other measures have been taken to ensure that the risk is no longer likely to occur again.

7.3. Notification process

The notification process will be carried out in several phases:

Investigation:

We will conduct a comprehensive internal investigation of the incident, identifying:

• the nature of the breach

• if possible, the categories and approximate number of individuals affected by the breach

• the categories and approximate number of personal data records affected;

• a description of the likely consequences of the data breach;

• a description of the measures taken or to be taken to prevent a recurrence of the incident or mitigate any potential negative consequences.

Protection:

We will immediately implement corrective measures to prevent the breach from continuing and/or recurring.

Information:

Those affected by the breach will be proactively informed, giving them the opportunity to take appropriate action.

They will be informed, as our investigations progress, of any useful information on the nature and extent of the Personal Data that may have already been affected and the corrective measures taken or planned to address it.

Notification:

If the breach poses a risk to an individual's rights and freedoms, a breach notification will be filed with the competent supervisory authorities, depending on the location:

- For personal data subject to Swiss law:

In accordance with Article 24 of the new Data Protection Act, which comes into force on September 1, 2023, data security breaches must now be reported to the Federal Data Protection and Information Commissioner (FDPIC) if they pose a significant risk to the personal or fundamental rights of the persons affected by the data breach. This reporting obligation applies to individuals, companies, and federal bodies and must be met as soon as possible using the reporting form here: https://databreach.edoeb.admin.ch/report

Submit a criminal complaint to the cantonal police at our headquarters; they will conduct the necessary investigations. Visit the website https://www.suisse-epolice.ch/#/search-station for nearby police stations and their contact details. Depending on where the company is located, the European Union's General Data Protection Regulation also applies when the leaked data is or includes personal data.

- For personal data subject to French and/or European legislation:

The notification will be sent to the CNIL as soon as possible following the discovery of a breach posing a risk to the rights and freedoms of individuals.

If we cannot provide all the required information within this timeframe because additional investigations are necessary, we will provide a two-stage notification:

1. An initial notification, if possible, within 72 hours following the discovery of the breach;

2. If the 72-hour deadline is exceeded, we will explain the reasons for the delay in our notification;

3. Finally, an additional notification as soon as additional information becomes available.

If we are a data processor, we notify the data controller of each data breach.

8. References

8.1. Legal framework

nLPD

Federal Data Protection Law (LPD) of September 25th, 2020 (FF 2020 7397).

https://www.fedlex.admin.ch/eli/fga/2020/1998/fr

8.1.1. Data Protection and Freedom Act

Law No. 78-17 of January 6th, 1978 relating to data processing, files and freedoms.

https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460

8.1.2. GDPR

The general data protection regulation – GDPR of May 23rd, 2018.

https://www.cnil.fr/fr/reglement-europeen-protection-donnees

8.1.3. Other regulatory references

For all information regarding other regulatory references, refer to the following sites:

https://entreprendre.service-public.fr/vosdroits/F10029#:~:text=Les%20livres%2C%20registres%2C%20documents%20ou,un%20d%C3%A9lai%20de%206%20ans.

https://www.fedlex.admin.ch/eli/cc/1999/354/fr