PERSONAL DATA MANAGEMENT POLICY
« GDPR »
FOR THE ALKALINE GROUP

1. OBJECT

The purpose of the personal data management policy (hereinafter referred to as "the policy") is to ensure that the processes handling personal data within the ALKALINE group (hereinafter "the company") comply with European provisions on the protection of personal data (EU Regulation 2016/679 hereinafter « GDPR »).

2. FIELDS OF APPLICATION

Companies majority owned by the company.

Any personal data processing including if this processing is carried out by a third party (hereinafter "subcontractor").

3. DEFINITIONS

Personal data: any information relating to an identified or identifiable physical person, whether directly (example: last name, first name) or indirectly (example: picture, telephone number), whether it is kept in digital or paper format. Data relating to legal entities are not concerned.

4. ACTORS

Data Protection Officer ("DPO"): The DPO is responsible for ensuring that the company complies with GDPR. He carries out risk assessments and leads the GDPR working group. He reports to the company's Management Committee.

The GDPR working group: It follows action plans, ensures communication on GDPR and awareness of teams, defines measures to reduce risks within the company.

IT Department: The IT department is responsible for the operation and security of IT systems and data. It plays an essential role in ensuring the security of personal data stored in computer format, in particular through hardware or software solutions and user training. He participates in risk assessments with the DPO.

Data controller: The data controller is the person who organizes the collection and processing of data.

Subcontractors: Subcontractors carry out data collection and processing on behalf of the company. They must also respect the rules for the protection of personal data entrusted to them or to which they have access.

The CNIL: The CNIL is the body responsible to monitor compliance with the GDPR. It can act as advisor for the activities based in France. It has the power to sanction.

Employees and managers: without necessarily being aware of it, any person in the company is likely to process personal data.

The Management Committee: the Management Committee supervises the activities of the DPO, allocates the resources necessary for its mission and defines its objectives annually.

5. GOALS OF THE COMPANY

5.1. Keep the data processing register up to date

The DPO maintains the register of data processing processes. This register is regularly reviewed by the working group to identify whether new treatment processes have been put in place.

5.2. Carry out an impact study on the processes handling personal data

For each treatment process appearing in the register, the DPO carries out a risk assessment using the PIA software made available by the CNIL.

The assessment covers the following points:

- The purpose of processing by verifying that it meets either a legal requirement or a business purpose which must be defined and lawful,
- The type of data processed, their sensitivity and their life cycle,
- Measures to protect the rights of individuals over their personal data,
- Risks that may lead to illegitimate access, loss or destruction of data,
- Existing measures to reduce these risks.

Each assessment is carried out jointly by the DPO and the IT department with the data controller.

Depending on the risk assessed on a severity / likelihood matrix, actions are decided (who, what, for when) with the data controller and the IT department to reduce the level of risk.

At the end of the assessment, the opinion of the DPO and the IT department is collected and noted in the register.

The assessment and the action plan are sent to the data controller and to the IT department.

The treatment plan of action is followed at each meeting of the working group. The metric used is the rate of progress of the actions decided.

In case of detection of personal data processing for which the purpose is unlawful, the DPO informs the Group management as soon as possible for a decision to be taken.

5.3. Communicate internally and externally

Sensitization of data controllers is carried out during risk assessments.

A quarterly update is presented by the DPO to the management committee with, in particular, monitoring of the progress of actions and of the most risky processes.

Company staffs are regularly informed of the progress of the GDPR process through the internal newspaper "Le Petit Messager".

The policy is also published on the website www.metauxspeciaux.com.

Appropriate communication is also sent to our shareholder.

5.4. Train

A staff training module on GDPR will be developed by the DPO who will ensure its presentation during IT security training sessions to be provided by the IT department. If the DPO is unable to attend, this training may also be led by another member of the working group.

5.5. Make sure subcontractors comply with GDPR.

The company checks that subcontractors who process personal data are contractually committed to processing this data in accordance with the GDPR. It checks whether the contractual obligations of the subcontractors guarantee a sufficient level of protection.

A high level of vigilance is focused on IT subcontractors who have access to a large amount of data (software publishers, service providers, cloud hosting solutions, SAS

mode services, data hosts), as well as only to subcontractors and suppliers hosting data outside the European Union.

In case of doubt about the security level of a subcontractor, an audit can be carried out by the DPO and the IT department.

5.6. Respect the rights of individuals

The company undertakes to inform individuals (employees, customers, suppliers, third parties) of the personal data it holds on them, of the purpose of the processing and of their right of access to these data, to rectify and of erasure.

When the processing is not linked to a legal or contractual obligation, the company also undertakes to obtain the consent of individuals on the use that will be made of their personal data. The consent is collected by the data controller, after consulting the DPO, and proof of this collection is kept by the data controller.

5.7. Improve IT good practices

Following GDPR assessments and IT security audits, the IT department has implemented:

- For newcomers: an IT welcome course for newcomers with advice on raising awareness of IT security and signing the IT charter;

- For staff already present in the company: a computer security awareness program and mouse pad recalling best practices in IT security.

5.8. Define archiving duration

Refer to company's internal procedure.

5.9. Intervening upstream in projects to guarantee the security of personal data

The DPO may be requested by the data controller beforehand for any project involving new processing of personal data. It analyses the planned treatment, the data collected and makes recommendations to the data controller.

Likewise, the DPO may be called upon by any employee on matters of personal data protection (files, etc…).

5.10. Securing the transfer of personal data outside the European Union

As part of an international group, the company sends documents containing personal data to entities located outside the European Union.

Standard contractual clauses between the company and the legal entity receiving the data are established, in accordance with the recommendations of the CNIL.

5.11. Inform CNIL in case of breach of personal data

The company will inform the CNIL within 48 hours in the event of illegitimate access to data brought to its attention. The company will verify that this obligation is included in the contractual obligations of its subcontractors.