Elemental Holding SA

Personal Data Protection Policy

applicable in the Elemental Holding Capital Group

VERSION: 1.0

DATE OF ISSUE: 15 May 2018

APPROVED BY RESOLUTION OF THE MANAGEMENT BOARD OF ELEMENTAL HOLDING S.A.

of 15 May 2018 No. 01/05/2018

§1. General provisions

1. This Personal Data Protection Policy, hereinafter referred to as the “Policy”, defines the purpose, legal basis and scope of processing personal data in Elemental Holding S.A. (hereinafter referred to as the “Company”) and in the Elemental Holding Capital Group (hereinafter referred to as the “Capital Group”), as well as information on entities to which data may be made available and on the rights of persons whose data are processed.
2. The policy is public and generally available, in particular it is published on the website of Elemental Holding S.A. www.elemental.biz, it may also be made available at the request of a person concerned.
3. Companies from the Capital Group ensure security of personal data entrusted to it based on:
   a) legality – companies protect their privacy and process data in accordance with the law;
   b) security – companies ensure an adequate level of data security by constantly taking actions in this respect.
   c) rights of an individual – the companies allow persons whose data they process to exercise their rights and implement these rights;
   d) accountability – the companies document how they fulfill their obligations to be able to demonstrate compliance at any time.
4. The following principles apply to personal data processing in the Capital Group:
   a) legitimacy – actions in the field of personal data processing must have a legal basis,
   b) reliability,
   c) transparency – processing is carried out in a way transparent for the data subject,
   d) minimalism and adequacy – data are collected for specific purposes, only to the extent that they are needed for a given purpose,
   e) accuracy – with attention to data accuracy,
   f) timeliness – for no longer than necessary;
   g) security – ensuring adequate data security.

§2. Personal data protection system

1. In order to implement the above principles, the following activities are carried out in the Capital Group:
   a) personal data are subject to identification: verification of the types of personal data processed, taking into account data classes (ordinary data, sensitive data), relationships between data resources, data profiling, co-administration, cases of entrusting the processing of personal data,
   b) a register of processed personal data is kept,
   c) legal basis for data processing is identified, verified and registered in the register, in particular a management system of data processing consents is maintained, and cases where data are processed on the basis of the legally justified interest of a Capital Group company are recorded and substantiated,
   d) companies from the Capital Group fulfill information obligations towards persons whose data they process and provide support for their rights by implementing requests received in this regard, including:
      i. during the process of obtaining consent for the processing of personal data, they provide information clauses explaining data processing principles adopted in a given company from the Capital Group and the scope of rights vested in a person entrusting his/her data,
      ii. they document the process of obtaining consent for the processing of personal data,
      iii. they verify and ensure a possibility of exercising rights of entitled persons in the scope of their personal data as part of their activities as an administrator, as well as processors entrusted with the processing of personal data,
      iv. they use procedures to determine the need to notify persons affected by an identified data protection breach,
   e) companies from the Capital Group have implemented the privacy by default principle, adopting the principle of data adequacy management; the principle of rationing and managing data access; the principle of managing the period of data storage and verification of further suitability,
   f) companies ensure an adequate level of data security, including:
      i. they carry out risk analysis for data processing activities or their specific categories;

ii. they carry out an assessment of impact on data protection where the risk of violating rights and freedoms of persons is high;
iii. they adapt data protection measures to a specified risk;

g) a security policy for the processing of personal data has been adopted in the Capital Group.

2. Companies from the Capital Group entrust processing of personal data to entities which have been verified in terms of compliance with personal data safety procedures. Processing of personal data is entrusted based on processing contracts regulating the required level of data security in accordance with the principles adopted in the Capital Group.
3. Companies from the Capital Group do not transfer data to third countries or international organizations.
4. Companies from the Capital Group manage changes that affect privacy. To this end, procedures for launching new projects and investments take into account the need to assess the impact of changes on data protection, ensuring privacy (and compliance of processing purposes, data security and minimization) already at the design stage of a change, investment or at the beginning of a new project.
5. Companies from the Capital Group do not conduct cross-border processing of personal data.

§3. Processing basis

1. Each of the companies from the Capital Group documents legal grounds for data processing for individual processing activities in a register.
2. Companies from the Capital Group implement methods of managing consents that enable registration and verification of a person's consent to process specific data for a specific purpose and registering refusal of consent, withdrawal of consent and similar activities (objection, restriction, etc.). In the process of obtaining consent, the companies inform in detail of rights of an individual regarding a given type of consent.
3. The companies from the Capital Group care about the clarity and style of information and communication with people whose data they process.
4. Companies from the Capital Group care about keeping legal deadlines for fulfilling their obligations towards persons whose data they process.
5. Companies from the Capital Group introduce adequate methods of identification and authentication of persons for the purposes of exercising individual rights and performing information obligations.

6. In order to exercise rights of an individual, the Capital Group companies provide procedures and mechanisms to identify data of specific persons processed by a respective company, integrate the data, amend and erase them in an integrated way,
7. Companies from the Capital Group document the handling of information obligations, notifications and requests of persons.

§4. Information duties

1. Companies from the Capital Group define legal and effective means of performing information duties, in particular they inform a person about the principles of data processing when obtaining data from that person.
2. Companies from the Capital Group define the manner of informing people about the processing of unidentified data, where it is possible (e.g. a plate informing that the area is covered by video surveillance).
3. Companies from the Capital Group inform a person about a planned change of the purpose of data processing.
4. Companies from the Capital Group inform a person before revoking a processing restriction.
5. Companies from the Capital Group inform data recipients about rectification, erasure or restriction of data processing (unless it requires a disproportionately large effort or is impossible).
6. Companies from the Capital Group inform a person about his/her right to object to the data processing not later than at the first contact with that person.
7. Companies from the Capital Group notify a person about violation of personal data protection without undue delay, if it may cause a high risk of violating rights or freedoms of that person.

§5. Implementation of rights

1. In implementing rights of data subjects, companies from the Capital Group introduce procedural guarantees to protect rights and freedoms of third parties. In particular, when reliable information is received that compliance with a person's request for a copy of data or the right to transfer data may adversely affect rights and freedoms of others (e.g. rights related to protection of other people's data, intellectual property rights, trade secrets, personal rights, etc.), the company may ask such person to clarify doubts or take other legal steps, including refusal to comply with the request.

2. At the request of a person regarding access to his/her data, a company from the Capital Group informs the person whether it processes his/her data and informs the person about processing details in accordance with Article 15 GDPR (the scope corresponds to the information obligation when collecting data), and also gives the person access to data concerning him/her.
3. A company from the Capital Group informs a person, within one month of receiving a request, of refusing to consider the request and the person's rights related thereto.
4. A company from the Capital Group rectifies incorrect data at the request of a person. The company has the right to refuse to rectify the data, unless the person shows irregularity of the data rectification of which he or she demands in a reasonable manner. In the case of rectifying such data, the company informs the person about data recipients, if requested by that person.
5. A company from the Capital Group supplements and updates data at the request of a person. The company has the right to refuse to supplement the data if the supplement would be inconsistent with the purposes of data processing (e.g. it does not have to process data that it does not need). The company may rely on a statement of the person regarding the data being filled in, unless it is insufficient in the light of the adopted procedures (e.g. with regard to collecting such data), the law or if there are grounds to consider the statement unreliable.
6. At the request of a person, a company from the Capital Group erases data when:
   a) the data are not necessary for the purposes for which they were collected or processed for other purposes,
   b) the consent for their processing has been withdrawn and there is no other legal ground for processing,
   c) the person has filed an effective objection against the processing of such data,
   d) the data were processed in an illegal way,
   e) the necessity of erasing results from a legal obligation,
   f) the request relates to child's data collected on the basis of consent to provide information society services directly offered to the child (e.g. a child's profile on the social network, participation in a competition on a website).
7. The Capital Group defines the manner of handling the right to erase data in a way ensuring effective implementation of this right, while respecting all data protection principles, including security, as well as verifying whether there are exceptions

referred to in Article 17 section 3 GDPR. In the case of data deletion, the company informs the person about data recipients, if the person requests so.

8. If the data subject to erasure have been made public by a company from the Capital Group, the company undertakes reasonable actions, including technical measures, to inform other administrators processing such personal data about the need to erase the data and access thereto.
9. A company from the Capital Group limits data processing at the request of a person when:
    a) the person questions data correctness - for a period that allows checking their correctness,
    b) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead,
    c) the company no longer needs personal data, but they are needed by the data subject to establish, pursue or defend claims,
    d) the person has objected to the processing for reasons related to his/her specific situation, until it is established whether the company has a legitimate interest overriding grounds of objection.
10. During the processing restriction, the Company stores data but does not process them (does not use them, does not transmit them) without the consent of the data subject, unless in order to establish, pursue or defend claims, or to protect the rights of another natural or legal person, or on serious grounds of public policy.
11. In the case of restricting data processing, the company informs the person about the recipients of the data, at the request of that person.
12. At the request of a person, a company from the Capital Group issues in a structured, commonly used machine-readable format or transfers to another entity, if possible, data about that person that he/she has provided to the company, processed on the basis of the person's consent or in order to conclude or perform an agreement concluded with that person, in the company's IT systems.
13. If a person opposes to the processing of his/her data due to his/her particular situation and the data are processed by the company based on its legitimate interest or tasks entrusted to the company in the public interest, the company will take into account the opposition unless the company has legitimate grounds for processing that override the interests, rights and freedoms of the opponent or the basis for establishing, pursuing or defending claims.

14. If a person opposes to the processing of his/her data by a company from the Capital Group for direct marketing purposes (including profiling, if any), the company will comply with the opposition and discontinue such processing.
15. Companies from the Capital Group do not profile a person in order to take a decision with respect to that person that has legal effects or otherwise significantly affects the person.

§6. Access restrictions

1. Companies from the Capital Group apply the following restrictions on access to personal data: legal (confidentiality obligations, authorization limits), physical (access zones, closing premises) and logical (restriction of rights to systems processing personal data and network resources which platform personal data).
2. Companies from the Capital Group update access rights in the case of changes in the composition of staff and changes in the roles of persons, as well as changes in processing entities.
3. Companies from the Capital Group periodically review established system users and update them according to their needs.
4. Detailed rules for controlling physical and logical access are included in the security procedures for personal data processing adopted by companies from the Capital Group.

§7. Minimizing time

Data whose usability gets reduced along with time by are removed from the systems as well as from the working and main files. Such data can be archived and be located on backups of systems and information processed by a company from the Capital Group. Procedures for archiving and using archives, creating and using backup copies take into account the requirements of controlling the life cycle of data, including the requirements for data erasure.

§8. Reporting violations

Companies from the Capital Group apply procedures to identify, assess and report an identified data breach to the Data Protection Authority within 72 hours of establishing the breach.