GDPR COMPLIANCE POLICY

Purpose

This Policy is the document regulating the activities of Softline Group in the field of compliance with the most relevant and specific requirements of Regulation (EU) 2016/679 (General Data Protection Regulation, "GDPR").

The purpose of this Policy is to ensure protection of data subject's rights and interests, which will result in Company's safety in the face of statutory liability and integrity of commercial operations.

General Provisions

This Policy applies to all Softline Companies and staff members.

Staff members shall:
- read, understand and comply with this Policy and any other documents designed to implement this Policy;
- receive the required training, including training courses and instruction;
- give notice of the requirements of this Policy to Business Partners.

Managers shall:
- ensure that staff members and Business Partners follow the requirements and instructions of this Policy.

The Compliance Service/Compliance Director shall:
- update this Policy and any other documents designed to implement it, as appropriate;
- provide staff members and Business Partners with advice and support regarding compliance with the requirements of this Policy and the law.

This Policy is not intended to replace existing security policies.

Terms and Definitions

Personal Data means any information relating to an identified or identifiable individual (data subject); an identifiable individual is a person who can be identified directly or indirectly, in particular through identifiers such as name, identification number, location data, online identifier, as well as one or more characteristics specific to the physical, physiological, genetic, mental, economic, cultural or social identity of this individual.

Data 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 of personal data.

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

Data Processing Principals

Lawfulness, fairness and transparency – personal data should be processed lawfully, fairly and in a transparent manner. The best way to comply with this principle is to assess data processing activities from the perspective of data subject's view and its expectations.

Purpose Limitation – personal data should be collected for specified, explicit and legitimate purposes. The best approach to comply with this principle is to avoid general categories of purposes and identify the purposes as specifically as possible.

Data minimization – personal data processed should be adequate, relevant and limited to what is necessary in relation to the specified purposes for which they are processed. Whenever possible, personal data should be anonymized or pseudonymised at the earliest opportunity. Each data asset processed by the Company shall be evaluated and reduced to the extent strictly necessary for the specific purpose of processing. When the data is no longer needed for the purpose for which it was collected, and if there is no lawful basis for continuing to keep it, the personal data must be either fully anonymized or deleted.

Accuracy – personal data processed should be accurate and, where necessary, kept up to date. Any new data regarding a data subject shall be recorded in a way to clearly identify its accuracy and relevancy.

Integrity and confidentiality – personal data should be processed in a manner that ensures appropriate security of the personal data including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Data Security Principles

Systemic approach. All Company assets are considered to be interrelated and mutually influencing components of a single system. In case of information security threats, the maximum possible amount of system behavior scenarios shall be taken into the account. The protection system is built taking into account not only all known channels of obtaining unauthorized access to information, but also considering the possibility of appearance of fundamentally new ways to implement security threats.

Complexity approach. A wide range of measures, methods and means of information protection shall be used in order to ensure information security. Their complex using implies the coordination of heterogeneous means in constructing the integrated protection system which blocks all the existing channels of threats and containing no weaknesses at the junctions of its separate components. The Company shall take effective measures and procedures to verify data security in both electronic communications and non-automated data operations in Company's physical premises.

The separation principle. One cannot rely on a single protective line, no matter how safe it may seem. Data security system shall be constructed in such a way that the most protected security zone is placed inside other protected zones. The data shall be stored and processed in the manner which provides safety of each data asset in case of security breach of other data assets.

The principle of equal strength. The effectiveness of protection mechanisms must not be reduced to nothing by a weak link, arising as a result of underestimation of the real threats or the use of inadequate protection measures.

The principle of continuity. The Company shall ensure that information security is a continuous and purposeful process, which implies taking the appropriate measures at all stages of the data asset lifecycle.

The principle of reasonable sufficiency. The Company assumes that it is impossible to create an absolute protection of all data assets. Therefore the choice of means of assets protection must be adequate to real existing threats and sensitivity of each specific data asset.

The controllability principle. All data security management and assurance processes in the Company must be controlled, i.e., it should be possible to monitor and measure the processes and components, to identify in time the information security violations and to take appropriate measures.

The principle of personal responsibility. Each employee is responsible for ensuring the safety of assets within his disposal.

Data Protection by Design and by Default

Implementation of these principles is controller's responsibility. However, processor is involved into implementation within controller's compliance policies and procedures.

General requirement resulting from these principles is to take into account the data subject's protection, interests and processing expectations during the whole processing lifecycle. The data subjects shall be free to take decisions on the processing of their data. These principles shall be implemented by default and shall not require the data subject to provide any additional actions to implement them.

Specifically, the data processing activities shall be organised in a manner which prevents public disclosure either by default or by incident without the same intention of the data subject.

The customer base of the Company is stored in a manner which prevents third party access, or the employee data is available only to HR staff, or the software which contains personal data is password-protected. However, the person responsible for data protection in the Company shall take these principles into consideration during the audit of specific data processing activity.

Rights of data subjects

The right to withdraw the consent

If personal data are processed on the basis of the consent of the data subject, the data subject may withdraw it at any time without affecting the validity of the processing performed on the basis of consent of the data subject prior to its withdrawal.

The right for information

Upon the data subject's request the Data Controller shall provide information concerning the data relating to him, including those processed by a data processor on its behalf or according to his/her notice, the sources from where they were obtained, the purpose, grounds and duration of processing, the name and address of the data processor and on its activities relating to data processing, and the conditions and effects of the data incident and measures taken with a view to eliminate them and – in case of data transfer – the legal basis and the recipients.

Data Controller must comply with requests for information without any delay, and provide the information requested in an intelligible form, in writing at the data subject's request, within not more than twenty-five days.

The information shall be provided free of charge for any category of data once a year. Additional information concerning the same category of data may be subject to a charge. Where any payment is made in connection with data that was processed unlawfully, or the request led to rectification, it shall be refunded.

The right for rectification

The data subject may request to correct his or her personal data if they are inaccurate, incomplete or outdated. If untrue personal data and the data that correspond to the reality, is available for Data Controller, personal data shall be corrected by Data Controller.

The right for removal

The data subject may request to remove his or her personal data if:

- personal data is no longer required for data processing purposes;
- the data subject has withdrawn his or her consent to the processing of data processed exclusively on the basis of such consent;
- data subject expresses disagreement with data processing;
- personal data processing is illegal;
- personal data must be removed in order to fulfill the legal obligations assumed by the Company.

The Company will take reasonable steps to inform other persons to whom personal data have been transferred about the fact of the personal data removal.

The right to restrict personal data processing

The data subject may request to limit the processing in case:

- the correctness of personal data is disputed;
- the data subject wants to restrict access to their personal data, instead of removing them despite the fact that their processing is illegal;
- the data subject wants the Company to retain his or her personal data, because it is required for data subject to protect the data under any legal requirements;
- the data subject objected to the personal data processing, and the Company conducts an audit to establish the legal grounds sufficient to ignore the data subject's rights, taking into account that the data processing is based on the legitimate Company interests.

The right for portability

The data subject may require the transfer of his or her personal data, provided that the personal data processing is based on his or her consent or performance of the contract, and is performed using automatic means (without using written (paper) documents).

The right to object to processing

If a data subject objects against processing of personal data, relating to him or her, Data Controller the controller shall investigate the cause of objection within the shortest possible time inside a fifteen-day time period, adopt a decision as to merits and shall notify the data subject in writing of its decision.

If, according to the findings of the controller the data subject’s objection is justified, the controller shall terminate all processing operations (including data collection and transmission), block the data involved and notify all recipients to whom any of these data had previously been transferred concerning the objection and the ensuing measures, upon which these recipients shall also take measures regarding the enforcement of the objection.

If the data subject does not agree with the decision of Data Controller, or if Data Controller does not comply with the deadline for making the decision, the concerned person may refer the case to court within 30 days from the date of notification of the decision or from the last day of the deadline.

The indemnification right

If the Data Controller causes damage related to the illegal personal data processing or violation of data security requirements, it is obliged to compensate it.

If the Data Controller violates the personal right of the data subject as a result of illegal processing of his or her personal data or violates the data security requirements, the data subject may claim damages.

The Data Controller is also liable to the data subject for the damage caused by the Data Processors. The Data Controller is relieved of liability for damage and damages if it proves that the

damage or violation of the personal rights of the data subject is caused by an unavoidable reason that goes beyond data processing.

Compensation is not required and the damage cannot be claimed when the damage caused to the injured party or the violation of the right to privacy was caused by the intentional or gross negligent behavior of the relevant data subject.

The right for court protection

The concerned person may claim to the court for violation of his or her rights. Data Controller shall demonstrate that the data is processed in accordance with the law. The claim may be filed by the concerned person in his or her own behalf to the competent court at the place of residence or habitation.

If the court satisfies the claim of the data subject, Data Controller is obliged to provide information, correct, block, remove, decrypt the automated data processing, taking into account the right to object of the relevant person.

The right to apply to the Personal Data Protection Authority

In case of any problems with the personal data processing conditions, the data subject can also file a complaint to supervisory authority of personal data protection.

Global CEO

Sergey Chernovolenko